Surveillance with non-purpose built technology

Milaj, Jonida

university of groningen

Surveillance with non-purpose built technology

Challenges for the protection of the right to privacy in the European Union

PhD thesis

to obtain the degree of PhD at the
University of Groningen
on the authority of the
Rector Magnificus Prof. E. Sterken
and in accordance with
the decision by the College of Deans.

This thesis will be defended in public on

7 September 2017 at 14.30 hours

by

Jonida Milaj-Weishaar

born on 30 March 1980
in Fier, Albanië

Supervisor
Prof. G.P. Mifsud Bonnici

Co-supervisor
mr. dr. A.M. Klingenberg

Assessment Committee
Prof. J.A. Cannataci
Prof. N. Forgó
Prof. A.L.B. Colombi Ciacchi

Acknowledgements

"*If we knew what we were doing, it wouldn't be called research, would it*?" This quote attributed to Albert Einstein aptly describes the writing process this manuscript went through. When I started to work on the topic I was very much fascinated by the many stories I heard and read in the media on amazing technologic developments which were quickly leaving behind any legal and regulatory framework. Today, having completed this research, I am convinced about the role that legal rules and principles can and should play for protecting individuals from the powers that technology gives to various actors and especially the State. This research made me realize that if technology is easy to escape legal rules, the way we employ technology, should not. Fortunately, during this process I wasn't alone. I had the guidance and the support of many people to which my deepest gratitude goes.

This work would have not been possible without the trust, constant guidance and support that Professor Mifsud Bonnici afforded me. During these years, Jeanne has not only been a great supervisor but also a role model in kindness and, above all, in dedication. I would also like to thank Aline Klingenberg, my second supervisor, for her guidance and support and for bringing to our discussions a new level of concreteness based on national administrative practices. I would like to thank Professor Gormley and all the former and present members of the department of European and Economic law for all the inspiring discussions and exchange of ideas. I also would like to thank all my colleagues at the Security Technology and e-Privacy (STeP) research group. I am not listing all their names one by one but I cannot deny that their energy, motivation, dedication, jokes and informal discussions have been a true source of energy and inspiration during all these years.

This work would have also not been possible without the unconditional love and support of my big and small family. I would like to thank my parents and my parents in law, my brother Enklid, as well as Aishe, Andreas and Anne, and my 3 nieces and nephew that, even if distant, have always been there for me in various ways. I would also like to thank my cousin Robert who was taking the picture that is now on my cover page. Last but not least, this work is dedicated to Stefan and Luís - without whom, no work would ever be complete.

Table of Contents

Chapter 1 Introduction

"Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."[1]

1.1 Background of the study

The television set can now listen to what we are saying. The label of the newly bought t-shirt we are wearing may trace our itinerary around the city. The camera of the computer can be remotely turned on and record all that happens in the room. The smart phone carried in the backpack discloses our presence at that political gathering on a Saturday afternoon. These are just some random examples of what technology is able to do. It is not a scoop anymore to read such stories and many more on the daily news. The devices that surround us make our world dominated by extensive and ubiquitous surveillance. We are all under some form of passive surveillance since data on our daily activities and interests is systematically collected due to the new advanced technology that we use.[2] It goes even further. We are not in control of the devices that we handle. We cannot turn them completely off. They are always there, watching, listening, smelling, and we never know who is at the other end. Many devices that are not built for the purpose of surveillance are still ready to surveil us. The internet of things age in which we live challenges the safeguards to our fundamental right to live an undisturbed private life and raises questions on its proper protection.[3]

The situation in which we find ourselves today has different reasons. Partly it is linked with the monetary value that personal information has. Companies are incentivized to create devices that collect data because it helps them to make money. Not without a reason in 2009 the than European Consumer Commissioner, Meglena Kuneva, defined personal data as "[…] *the new oil of the internet and the new currency of the digital world*."[4]

The possibility that devices have for collection and retention of personal data opens the doors to potential disclosures of these data that were not anticipated at the initial moment in which they were collected. The data can be passed on or sold to third parties. Sometimes these third parties can be other companies, but can also be governments and law enforcement agencies. Collected and

[1] Justice Brandeis dissenting opinion in Olmstead v. United States, 277 U.S. 438 (1928)

[2] McCullagh D., Broache, A. (2006) FBI taps cell phone mic as eavesdropping tool, *CNET News*, December 2006, available at: http://news.cnet.com/2100-1029-6140191.html (last accessed: 29.7.2016); Lyon, D. (2007) Surveillance, power and everyday life, available online at: http://www.sscqueens.org/sites/default/files/oxford_handbook.pdf (last accessed: 29.7.2016)

[3] GPEN (2016) Privacy SWEEP on IoT, available online at: https://www.privacyenforcement.net/press-releases (last accessed: 9.11.2016), the data revealed that 60% of devices are not in conformity with privacy and data protection rules

[4] Kuneva, M. (2009) Keynote Speech at Roundtable on Online data collection, targeting and profiling, Brussels 31 March 2009, Speech/09/156, available online at: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (last accessed: 26.7.2016)

retained data have a potential to be used for crime control giving law enforcement the possibility to retrieve historical data on individuals, once they become suspects.[5] The new technology enables law enforcement to even access historical data that they could not have been able to obtain in real time without having the individuals under continuous surveillance.[6] A well-known example of such an activity in Europe was the introduction of an obligation for telephony and internet companies to make available communication metadata, that they would normally collect for various purposes (e.g. billing), to law enforcement for the purpose of prevention, detection, investigation and punishment of serious crime.

Technology running too fast ahead of the laws is the other reason for the surveillance reality in which we find ourselves today. The legal architecture, nationally and internationally, has not anticipated the challenges that the development of technology would present for the protection of the fundamental rights of the individuals. As a result, confronted with the benefits of technology, individuals´ fundamental rights are often unprotected.

The use for surveillance of devices that are not built for that purpose is making such an activity ubiquitous. In addition, the collection and retention of data that is not predestined for a specific use is too indiscriminate and thus violates the right to privacy. Without proper guarantees and limitations, it may amount to "complete surveillance".[7] As a result, the European legal framework designed in the light of the traditional forms of surveillance is challenged by the new technology able to obtain the same or similar information without the need of any physical intrusion into private premises. No physical intrusion, however, does not make the new technology less dangerous for the violation of the fundamental right to privacy of the individuals.

While the problems that technology with a potential to be used for intruding privacy are recognized for third countries with a weak protection of human rights,[8] we are still lacking a comprehensive study on the effects that the use of such a technology by law enforcement has for the individuals in the European Union. This is the gap that this study addresses focusing on human rights implications of technical advances that threaten to emancipate from both the existing legal regime as well as current scholarship.

---

[5] Töllborg, D. (1995) Undercover in Sweden: The Swedish security police and their modus operandi, in Fijnaut, C., Marx, G.T. (eds.) *Undercover: Police Surveillance in Comparative Perspective*, pp. 248-268; Brouwer, E. (2007) The use of biometrics in EU databases and identity documents, in Lodge, J. (eds.) *Are you who you say you are? The EU and Biometric Borders*, pp. 45-66

[6] Bellia, P.L. (2008) The memory gap in surveillance law, *University of Chicago Law Review*, vol. 75, no. 1, pp. 137-179

[7] Rushin, S. (2011) The judicial response to mass police surveillance, *Journal of law, technology and policy*, no. 2, pp. 281-328

[8] European Parliament (2015) European Parliament resolution of 8 September 2015 on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries' (2014/2232(INI))

1.2 The focus of the research

This research focuses on the law enforcement use of devices which are not originally built for the purpose of surveillance and the challenges that this presents for the protection of the right to privacy. Intelligence structures are thus outside the scope of the research. This is a legal study and as such it focuses on the legal architecture at European Union level and it analyses its adequacy or failure to protect the rights of the individuals in such situations.

Though law enforcement surveillance is mainly a national activity, the protection of the rights to privacy and data protection is regulated at European level. The European policy maker has already introduced a number of legal acts that aim for the exchange of data and information between the Member States for the scope of fighting criminal activities. These legal acts have to do, for example, with the exchange of information between law enforcement authorities,[9] the exchange of criminal records,[10] exchange of information between authorities responsible for prevention and investigation of criminal offences[11] and more recently also regulating data protection standards when personal data are processed nationally for the scope of prevention, detection, investigation and punishment of criminal activities.[12] This body of acts at European level suggests for the existence of common standards for the protection of the rights to privacy and data protection while still leaving to the Member States some margin of manoeuvre. Hence a study of the legislation and of the standards that apply to surveillance with non-purpose built technology at European level is highly justified.

Inspired by a human rights' based approach, which requires human rights standards to guide the reaching of measurable goals, this study aims to analyse the adequacy of the current European legal framework for addressing the challenges that surveillance with non-purpose built technology presents and to suggest potential solutions from a legal point of view.[13] As such, this work does not aim to an impracticable and unlikely result as it would be, for example, the suggestion for prohibiting law enforcement from using non-purpose built devices for the purpose of surveillance. The

[9] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, pp. 89–100

[10] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93, 7.4.2009, pp. 23–32

[11] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, pp. 1-11

[12] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[13] For a comprehensive definition of a "rights based approach" see: Collins, T., Pearson, L., Delany, C. (2002) Rights-based approach, Discussion paper available online at: http://03559de.netsolhost.com/htmfiles/hill/17_htm_files/Committee-e/Tara-ARightsBased.pdf (last accessed: 10.2.2017)

employment of such devices is certainly facilitating the activity of law enforcement authorities logistically, technically, economically, etc. However, it must be kept in mind that while the fight against crime is certainly in the public interest, it must not interfere with the fundamental rights to privacy and data protection beyond what is considered as necessary and proportionate in a democratic society.

Often, in the doctrinal debate, the protection of privacy is seen to weigh less than the security of the individuals (the latter understood as national security).[14] Certainly, security in the form of physical survival is a pre-requisite for enjoying any other rights, including the right to privacy. Such a debate is fuelled from some of the most aggressive and intensive terrorist attacks that the world is facing in the 21st century. In Europe, policy documents such as the Stockholm Programme[15] and the 5-year internal security strategies seem to present a trade-off model which supports security at the expenses of privacy.[16] Undoubtedly, when terror and crime override the structures of a democratic society it is difficult to strive for a different balance.

The new Data Protection Package that was adopted in 2016 at EU level presents two different legal instruments for dealing with personal data when used, for example, in a commercial relationship or for law enforcement purposes. The legislators' choice for not using the general regime in cases of law enforcement shows not only the specificity of the field but also covers up the use of a double standard when dealing with personal data. The protection of the rights of the individuals seems to be lower when their personal data are used for law enforcement purposes.

For the individuals, however, the outcome of the debated privacy versus security discussion in such a context cannot be straightforward. In a 2014 survey on the desired level of surveillance in the means

[14] Chandler, J. (2009) Privacy versus National Security: Clarifying the Trade-off, in Kerr, I., Lucock C., Steeves, V. (eds.) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, pp. 121-138; Bigo, d., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf (last accessed 1.11.2013); De Hert, P. (2005) Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, vol. 1, no. 1, pp. 68-96

[15] The Stockholm Programme — An open and secure Europe serving and protecting citizens, OJ C 115, 4.5.2010, 1-38

[16] Fuchs, C. (2013) Privacy and Security in Europe*, The Privacy & Security-Research Paper Series*, Research Paper no. 6, available online at: http://www.projectpact.eu/privacy-security-research-paper-series/privacy-security-research-paper-series/6_Privacy_and_Security_Research_Paper_Series.pdf (last accessed: 28.7.2016)

of public transport, the European citizens showed that their preferences are much more nuanced than a straightforward inverse relationship.[17]

In this work, the fundamental right to privacy and the striving for the security of the citizens are not seen as two competing rights. Since both rights are designed for the enjoyment of the individuals in a democratic society they must not come at the cost of each other. Thus, this study does not advocate *ex ante* in the favour of any of them. Security while protecting privacy, and thus the existence of legal, administrative, and technical controls that make the use of technology for surveillance appropriate and accountable in a democratic society, is the underlying focus of this research

1.3 Research questions

The technological progress with all its positive benefits has also given to our society the characteristics of a big Panopticon structure as theorized by Bentham in the late eighteenth century.[18] To give just an example - in the UK it was disclosed the fact that law enforcement routinely sweeps up identities of thousands of people by simply requiring the mobile phone network information about all mobile phones connected to a certain cell tower at a specific time.[19] This form of processing location data for thousands of individuals clearly shows how their private lives are interfered with due to the technology that they carry with them as well as due to a failure in enforcing their rights.

This study starts from the presumption that, even if the way in which the private life of individuals is interfered with non-purpose built technology (defined in chapter 2) differs from the traditional ways of surveillance that law enforcement uses, non-purpose built technology used for surveillance has comparable capabilities and is at least as intrusive as traditional surveillance, if not more. Therefore, surveillance with non-purpose built technology might require to be subject to at least the same legal safeguards as traditional surveillance.

The legal framework at European Union level that applies to surveillance with non-purpose built technology is thus analysed for the first time in the present study. It assesses if the legal framework is accurately designed to address the presented challenges or if it needs to be adapted in order to secure for the individuals the protection of their fundamental right to privacy in a democratic society.

[17] Patil, S., Patruni, B., Lu, H., Dunkerley, F., Fox, J., Potoglou, D., Robinson, N. (2015) Public Perception of Security and Privacy - Results of the comprehensive analysis of PACT's pan-European Survey, available online at: http://www.rand.org/pubs/research_reports/RR704.html (last accessed: 28.7.2016)

[18] Foucault, M. (1979), Discipline and Punish – The birth of the prison, Vintage Books, New York, pp. 169-170

[19] King, E. (2012), Civil servant admits British police grabbing location data of thousands of innocent people, available at: https://www.privacyinternational.org/blog/civil-servant-admits-british-police-grabbing-location-data-of-thousands-of-innocent-people (last accessed: 1.8.2016)

Since the law usually lags behind technological developments, it is important to find ways for ensuring the safeguarding of the fundamental rights of the individuals in all situation.[20]

Within this framework, the central research question that this study answers is:

Is the European legal framework providing adequate protection of the fundamental right to privacy of the individuals against the threats created by law enforcement's surveillance with non-purpose built technology?

This research question cannot be answered without addressing first a number of issues that are presented below in the form of sub-questions. Each of these sub-questions contributes to the answering of the central research question. The first sub-research question identifies and analyses the legal characteristics that differentiate traditional forms of surveillance from surveillance with non-purpose built technology. It gives the possibility to identify the potential legal challenges that surveillance with non-purpose built technology presents and to analyse if they differ from the cases of traditional surveillance. Building up on this differentiation gives the possibility in later stages of the study to evaluate in how far the legislation designed for traditional surveillance is able to regulate law enforcement surveillance with non-purpose built technology.

The second sub-research question analyses if the European legal framework that applies to traditional surveillance covers also the challenges that surveillance with non-purpose built technology creates. Building upon the first sub-research question, it gives the possibility to take a holistic approach into the legal framework that deals with surveillance and privacy at European level and to identify legal provisions and principles that apply to surveillance with non-purpose built technology.

The third sub-research question analyses if the current structures of access to information allow disclosure for the use and the scope of surveillance with non-purpose built technology. Since non-purpose built devices used for surveillance are in the hands of the individuals and the data that they collect is available also with service providers or other private parties, this sub-research question gives the possibility to evaluate the legality of law enforcement making use of the privately collected data.

The fourth sub-research question analyses if the current structures of surveillance oversight at European level adequately address also surveillance with non-purpose built technology. The addressing of this sub-question gives the possibility to assess if the way surveillance oversight

[20] Koops, B.J. (2010), Law, Technology, and shifting power relations, *Berkeley Technology Law Journal*, vol. 25, no. 2, pp. 973-1035

operates in cases of law enforcement surveillance is adequate for cases of surveillance with non-purpose built technology.

1.4 Methodology and approach

The main task of legal science is to identify and systematize the applicable law.[21] Having such a task as the starting point, the present research project goes one step further. It aims not just at the identification of the applicable laws and judicial decisions for cases of surveillance with non-purpose built technology, but also at the identification of the legal implications and potential unbalances created with the fundamental principles of a democratic society, and especially the right to a protected private life.

The research is, thus, designed in light of a problem and interest oriented approach and it will not limit itself to legal dogmatism, neither to a systematic study of examples from the jurisprudence. This is because, in addition to descriptive and explanatory aims, the study is delineated with a law reformist ambition in the background, so as to bring the law up to date with the technological progress for the best protection of the rights and interests of the individuals. In order to make the analyses and the findings concrete, selected case studies based on examples of technology not built for the purpose of surveillance are presented and analysed in light of the applicable legislation and case law to assess the implications that the use for surveillance of non-purpose built technology might create from a fundamental rights perspective. The main research method is inspired by a human rights' based approach which requires human rights standards to guide the reaching of measurable goals, as it is the fight against crime. The underlying hypothesis that derives from this approach is that while the work of law enforcement authorities and the fight against crime are certainly in the public interest, they must not interfere with the fundamental rights to privacy and data protection of the individuals beyond what it is necessary and proportionate.

This legal study is augmented by the presence of elements from other fields of study, as for example: computer and information science, sociology, philosophy, political science, etc. The presence of these elements is natural since they are closely related with the study of the technology developments as well as with the effects these have for the enjoying of the rights of the individuals. Insights from these fields of study are an added value to this research, though the author cannot claim to be an expert in any of these additional fields.

1.5 Sources

For addressing the research questions, it is important to work closely with the existing literature in order to collect information on traditional as well as on surveillance with non-purpose built

[21] Wahlgren, P. (2000), On the future of legal science, *Scandinavian Studies in Law*, vol. 40, pp. 515-525

technology, and to reflect upon the implications that the use of these systems may create. In addition, the analyses of the current legal regime, including the existing legislation and case law at European Union level, gives the possibility to assess the applicability of the present rules to the challenges offered by the new technology.

The sources used for this research consist first of all of conventional legal materials such as: treaties, laws, regulations, preparatory works, recommendations, judicial decisions and legal scholars' works and commentaries on surveillance systems as well as on their human rights implications. In addition, literature on the new technologies with a potential to be used for surveillance purposes as well as sociological and philosophical literature on the consequences of surveillance for the society and the open debate on governance and decision making is consulted.

1.6 Outline of the study

After setting the scene for this study in this introductory chapter, the following chapters are designed in line with the identified research agenda. Chapter 2 addresses the first sub-research question and is thus dedicated to a legal analysis of non-purpose built surveillance technologies. It defines non-purpose built surveillance systems and technology and highlights their potential legal implications. The characteristics of these systems are confronted with the ones of traditional surveillance in order to assess their potential similarities and differences from a legal point of view. The challenges that surveillance with non-purpose built technology presents to the right to privacy are assessed with the help of insights from the legislation, case law and the legal doctrine.

Chapter 3 addresses sub-research question 2 and contains an analysis of the current European legal framework dealing with the fundamental rights to privacy and data protection and covering issues of surveillance. It theoretically assesses if the legal framework is extended to surveillance with non-purpose built technology and if it adequately addresses the challenges that surveillance with non-purpose built technology creates for the protection of the right to privacy. Part of this chapter is dedicated to the discussion on the similarities and difference between the rights to privacy and data protection. This is relevant for understanding in how far data protection legislation addresses also privacy concerns.

Chapter 4 is dedicated to the study of three different non-purpose built devices that are or may be used by law enforcement for surveillance purposes. The case study analyses give the possibility to assess the theoretical findings of the previous chapters in a concrete way. While the number of non-purpose built devices and technology increases, the case studies are selected as representative of the large areas of personal autonomy: private life, family life, home and correspondence, as well as location and space as a new and emerging privacy dimension. The selected case studies are: (i) smart meters; (ii) smartphones; (iii) GPS devices. The potential of these devices and the challenges that each of them creates for the protection of the right to privacy of the individuals are discussed in separate sections.

Chapter 5 addresses sub-research questions 3 and 4. It discusses the law enforcement access to information collected with non-purpose built technology as well as the structures of surveillance oversight. A special treatment in this chapter is given to the proportionality principle and the role that this has for ensuring the compatibility of interferences with the fundamental rights. The methods for assessing the impact of technology with the right to privacy and data protection are discussed and a new method that will assist decision makers in issuing proportionate surveillance mandates is proposed.

Chapter 6 concludes by bringing together the research findings and answering the main research question. It presents a number of recommendations for law enforcement authorities and service provides so that surveillance with non-purpose built technology does not undermine the protection of the fundamental right to privacy for the individuals and the necessity and proportionality principles of a democratic society. Since the current path of development has created a disconnection between the technology and the laws regulating it and there are no doubts that technology is going to be ahead of static laws also in the foreseeable future, the chapter will present the principles that must guide surveillance with non-purpose built technology for bringing any interference with the right to privacy of the individuals into the realm of lawfulness and compatibility with human rights.

Chapter 2 Surveillance with non-purpose built technology

2.1 Introduction

The progress of technology, together with the innovation, advancement and facilitation of many processes, has brought into life new ways of surveilling individuals and interfering with their right to a protected private life. Every day we learn about new technologies with potential to reveal the unseen, to present the unknown and to discover the forgotten.[22] The information collected and accessed due to these technologies can be easily analysed and combined with other information, resulting in detailed knowledge about behaviour and preferences of individuals and resulting in an intensive intrusion into their private sphere. We are carrying with us, in our pockets, the best and most efficient surveillance technologies of the time (as for example smart phones).[23]

While in a classic context surveillance is considered as a vertical activity, linked with State authorities that in a democratic society should operate in accordance with the legally binding rules and principles, due to the new and advanced available technology this conceptualization of surveillance has changed. Surveillance with new technology is considered and performed more and more as a horizontal activity. Devices in the hands of individuals create the possibility for collection and access of the data by private parties that operate the systems running on them and most of the time the bulk of data is self-feed by the individuals in attempts to monitor themselves.[24] The ease that technology presents for collecting information on the private life of the individuals and for accessing it should, however, not lower the standards of safeguarding the fundamental rights of European citizens and especially the right to a protected private life.

The possibility for law enforcement authorities to use non-purpose built but surveillance-ready devices for the purpose of surveillance cannot be ignored. As already stated in the introductory chapter, the aim of this research is to analyse if the legal framework applicable at European Union level is adequate for safeguarding the fundamental right to a protected private life of the citizens in cases of State surveillance via non-purpose built technology. In order to analyse the adequacy of the

[22] See for example the newest developments on wireless brain–computer interface in Borton, D.A. et al. (2013) An implantable wireless neural interface for recording cortical circuit dynamics in moving primates, *Journal of Neural Engineering*, vol. 10, no. 2, pp. 16; Young, S. (2013) A wireless brain-computer interface, available online in: http://www.technologyreview.com/news/512161/a-wireless-brain-computer-interface/ (last check on 24.04.2013); Marx, G.T. (2006) Ethics of the New surveillance, *The information society: An international journal*, vol. 14, no. 3, pp. 171-185

[23] Keynote address of Ian Readhead (Chief Executive, Association of Chief Police Officers, UK) with the title "From practitioners to policy-formulation to practice: stakeholder involvement in determining surveillance policy", held in the second policy workshop of RESPECT project, "*Technology and crime: law, privacy and policy in the era of Big Data*", Barcelona, 17-18 September 2014

[24] Vaz, P., Bruno, F. (2003) Types of self-surveillance: from abnormality to individuals 'at risk', in *Surveillance & Society*, vol. 1, no. 3, pp. 272-291

law, a number of milestones have to be reached beforehand. This chapter addresses sub-research question one. It defines surveillance with non-purpose built technology and highlights its potential legal implications for the protection of the right to privacy. The way surveillance with non-purpose built devices is performed is contrasted against traditional surveillance (which is also duly defined in this chapter) in order to assess their similarities and differences from a privacy protection point of view. This would give the possibility at later stages of the research to assess in how far the legislation designed in light of traditional surveillance is able to regulate the challenges that surveillance with non-purpose built technology creates.

After this introduction, in section 2.2, surveillance with devices not built for the purpose of surveillance is defined. In section 2.2.1 devices not built for the purpose of surveillance are discussed on the basis of examples in order to identify the effects that they present to the protection of the right to privacy. Based on the identified problems, section 2.3 is dedicated to identified challenges that surveillance with non-purpose built technology presents to the right to privacy. In turn are discussed incidental surveillance (sub-section 2.3.1), mass surveillance (sub-section 2.3.2) and retroactive surveillance (sub-section 2.3.1). The main findings of the chapter are summarised in the concluding section 2.4.

2.2 Defining surveillance with non-purpose built devices

The term surveillance derives from the French language and literally refers to a close watch kept over someone or something.[25] For Wigan and Clarke (2006) the origin of 'surveillance' derives from the times of the French revolution.[26] The term is related with the systematic investigation or monitoring of the actions or communications of one or more persons.[27] In contemporary social and political sciences, surveillance refers to the "*process of watching, monitoring, recording, and processing the behaviour of people, objects and events in order to govern activity*".[28]

As seen above, in its broadest sense surveillance means 'to watch over' and this activity is not limited to pure observation.[29] For Foucault (1995) the Panopticon[30] was a system which aimed "*to induce in*

[25] As defined by the Merriam-Webster Online Dictionary
[26] Wigan, M., Clarke, R. (2006) Social impacts of transport surveillance, in *Prometheus: Critical studies in Innovation*, vol. 24, n. 4, pp. 389-403
[27] Bennett, C. (1996) The public surveillance of personal data: A cross-national analyses, in Lyon, D., Zureik, E. (eds.), *Computers, surveillance, and privacy*, pp. 237-259
[28] Jenness, V., Smith, D.A., Stepan-Norris, J. (2007) Taking a look at surveillance studies, in *Contemporary sociology: A Journal of Reviews,* vol. 36, no. 2, pp. vii-viii
[29] Watney, M. (2008) Understanding electronic surveillance as an investigatory method in conducting criminal investigations on the internet, available online at: http://www.isrcl.org/Papers/2008/Watney.pdf (last accessed 27.1.2014)
[30] The Panopticon is a type of building design, especially for penitentiary houses, that allows a single watchman to observe all inmates without them being able to tell whether or not they are being watched. The idea was published in a work of the philosopher Jeremey Bentham in 1787, available online at: http://www.ics.uci.edu/~djp3/classes/2012_01_INF241/papers/PANOPTICON.pdf (last check: 16.03.2015)

the inmate a state of conscious and permanent visibility that assures the automatic functioning of power".[31] In Foucault's model surveillance is connected with both observation and control.

Notions of surveillance have traditionally been concerned with the attentive watching of State actors like law enforcement authorities rather than the one of companies and individuals.[32] But in a postmodern age Bauman and Lyon (2013) have identified the spread of surveillance beyond the State watching that is often non-consensual to a sometime private surveillance, in which the subjects increasingly consent and participate. They define it as "liquid surveillance".[33] The two phenomena, State and non-State surveillance, are seen for this conceptualization of surveillance as deeply intertwined. They support each other in a complex manner that is often impossible to disentangle. This conceptualization of surveillance derives from the fact that at the outset technologies with a possibility to be used for surveillance –RFID chips, GPS trackers, cameras and other sensors, etc. - are used almost interchangeably by State and non-State actors.[34]

Apart the involvement of State or non-State actors, the use of technology for surveillance shows also that the notion of surveillance cannot be linked anymore with simple physical watching. Tanner (2014) describes nicely how State surveillance has changed due to the technology: "*When I visited East Germany all those years ago, I was not producing a continuous stream of electronic data about my activities. If the Stasi wanted to know more, they had to follow people and monitor conversations the old-fashioned way, perhaps by having agents sitting for long hours around cafes and restaurants, or tapping into phones. In the internet era, why send ten agents out to trail someone when electronic footprints stored by private firms provide a far richer portrait of that person's activities?*"[35]

From the above example one can deduce not only the fact that due to the technology the role of the State and of private actors are intertwined, but also that technology has turned surveillance in an non economically burdensome activity which can be easily performed. Thus, there are risks that it may extend to situations in which it is not strictly necessary. Hence the proper protection of the right to privacy of the individuals becomes even more relevant.

This study focuses on surveillance as an investigation and information gathering activity performed by the State for meeting different needs of law enforcement activities, as for example: prevention or

[31] Foucault, M. (1995) Discipline and Punish: The birth of the prison, Vintage Books, p. 195
[32] Richards, N.M. (2013) The dangers of surveillance, in *Harvard Law Review*, vol. 126, pp. 1934-1965
[33] Bauman, Z., Lyon, D. (2013) Liquid surveillance: A conversation, Polity Press, pp. 2-3
[34] Lyon, D. (2007) Surveillance studies: An overview, Polity Press, pp. 111-112; Lyon, D., (2007) Surveillance, power and everyday life, in Mansell, R., Avgerou, C., Quah, D., Silverstone, R. (eds.), The Oxford handbook of Information and Communication technologies, available online at: http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199548798.001.0001/oxfordhb-9780199548798-e-019 (last accessed: 12.2.2016)
[35] Tanner, A. (2014), What stays in Vegas, Public Affairs, New York, pp. xiv-xv

detection of crime, identification of the responsible persons, etc. It distinguishes further between traditional surveillance and surveillance with non-purpose built technology.

Under the definition of traditional surveillance for this study fall physical surveillance activities, as for example when watching someone with the free eye or listening a conversation through the key hole of a door, but not only. This author qualifies also surveillance performed with surveillance technology as traditional surveillance. Surveillance technology is defined as comprising all the technology and devices that are used for the purpose of surveillance as being their first scope. Said differently, all the technology and devices designed and built for the purpose of surveillance and including, for example, bugs, street cameras, wiretapping devices, etc. Traditional surveillance thus includes physical surveillance and surveillance performed with surveillance technology.

The aim of this study is, however, not to assess the challenges that are created to the right to privacy from surveillance devices, but the challenges that are created from devices that are not-built for the purpose of surveillance. For this study, surveillance with non-purpose built technology is defined as State surveillance via technology and devices that have not been built for the purpose of surveillance as their first scope. To say that a device is not built for the purpose of surveillance as its first scope might be a bit presumptuous. One certainly cannot exclude the existence of cases in which the design and development of a certain technology or device is supported by underlying interests of intelligence and law enforcement bodies. That is why for this study the definition of devices non-built for the purpose of surveillance is limited to those that are introduced in the markets for the performance of another activity which is not linked *prima facie* with surveillance. There are many examples of such devices. We have just to think of smart phones, GPS navigation systems, smart tv, smart meters, etc. For the purpose of this study it is the combination of the ability and of the official accreditation that determines the qualification of a device as not built for the purpose of surveillance.

The definition of non-purpose built devices used for surveillance can be explained with the example of smart phones. These devices are designed for facilitating the communication among individuals, so they are not originally designed for the purpose of serving as surveillance devices. They have, however, a big data-storage capacity that can be used for capturing activities of their users. They can store texts, pictures or videos. They collect in one place many distinct types of information that reveal much more in combination than any isolated record and the data can even date back for years. In traditional surveillance electrical taps were introduced on a telephone line or device and used for intercepting personal communications. Interception of communications for current smart phone devices does not require the introduction of a wire and is, however, not the only surveillance potential of the device. For example, smart phones on the basis of their applications or of a simple triangulation assessment can serve as location tracing devices.[36] Apart location tracking,

[36] King, E. (2012) Civil servant admits British police grabbing location data of thousands of innocent people, available online at: https://www.privacyinternational.org/blog/civil-servant-admits-british-police-grabbing-

contemporary smart phones allow users to access internet. Analysis of the online behaviour can disclose a lot of information on the private life of the individual. In addition to these known possibilities offered by smart phones, there have been cases (made public in the United States of America) were judges authorized the remote activation of the microphone of a mobile phone to serve as a portable bug.[37] The device therefore offers different possibilities for interfering with the private life of the individuals, by accessing the data collected as well as by direct surveillance. The level of intrusion into the private life of the individuals of each of these possibilities, offered by a single device, differs. Location tracking in public spaces,[38] where one is exposed to be watched by many persons is considered, for example, as being less intrusive than the interception of a personal communication.[39] Access to a single device (phone) might be used, however, for tracking both activities, even simultaneously (e.g. establishing the location of an individual while engaging in a personal phone conversation). A more detailed analysis of surveillance with smart phones is presented in Chapter 4.

Another example of technology not built for the purpose of surveillance but having such ability are smart energy meters. These devices are introduced and promoted due to the benefits they are expected to bring to the electricity supply industry and its customers. These devices can accurately measure the power use of each household and send such data to a central server. The data may, for example, reveal huge energy consumptions and therefore help to detect illegal activities such as the cultivation of narcotic plants, or broadcasting copyright protected materials in infringement of the rules.[40] On the basis of the customer data it is possible to also identify the devices that are present in a household and whether they are turned on and how often.[41] As a result the presence of someone at the home can be detected as well as the standard of life a family is able to support (relevant for example for tax authorities). German researchers found in 2011 that the data collected by the smart meters can go as far as to reveal the programs someone watches on TV.[42] Apparently, "*the amount of light and dark emitted on the display for individual frames is unique for each TV program and movie*".[43] Smart meters may serve in this way for surveillance purposes, observing a number of activities inside a home, and collecting data on the behaviour of the targeted individuals, as well as of

location-data-of-thousands-of-innocent-people (last check: 18.07.2013); Zhao, Y. (2000) Mobile phone location determination and its impact on intelligent transportation systems, in *IEEE*, vol. 1, no. 1, pp. 55-64

[37] McCullagh, D., Broache, A. (2006) FBI taps cell phone mic as eavesdropping tool, *CNet News*, available online at: http://news.cnet.com/2100-1029-6140191.html (last check: 27.04.2013)

[38] Uzun v. Germany, ECHR application no. 35623/05, 2 September 2010, paras. 68-69

[39] Wicker, S.B. (2011) Cellular telephony and the question of privacy, *Communications of the ACM*, vol. 54, no. 7, pp. 88-98

[40] See presentation by Carluccio, D., Brinkhaus, S. (2011) Smart hacking for privacy, in 28th Chaos Communication Congress: Behind enemy lines, available online at: https://www.youtube.com/watch?v=YYe4SwQn2GE (last accessed: 16.3.2015)

[41] McKena, E., et al. (2012) Smart meter data: Balancing consumer privacy concerns with legitimate applications, *Energy Policy*, vol. 41, pp. 807-814

[42] Mills, E. (2012) Researchers find smart meters could reveal favourite TV shows, *CNet News*, available online at: http://news.cnet.com/8301-27080_3-57364883-245/researchers-find-smart-meters-could-reveal-favorite-tv-shows/ (last accessed: 27.04.2013)

[43] Greveler, U., et al. (2011) Multimedia Content Identification Through Smart Meter Power Usage Profiles, available online at: http://epic.org/privacy/smartgrid/smart_meter.pdf (last accessed: 27.04.2013)

other members of their household. A more detailed analysis of surveillance with smart meters is presented in Chapter 4.

Just from the two examples above, of smart phones and smart meters, it is clear that even if not designed for the purpose of surveillance these devices may have the ability to facilitate different forms of surveillance and interfere with the private life of the individuals in different ways. One way of interference is direct surveillance, i.e. surveillance on the spot or interference by the State on the device or network of a service provider.[44] The other way of interference is dataveillance,[45] i.e. surveillance of the track of data that someone leaves behind, though at times due to the very short intervals in which the data are transferred the distinction between direct surveillance and dataveillance blurs. Dataveillance opens the possibility to use for the purpose of surveillance personal data that have been collected by devices and systems for other purposes, as for example for billing transparency purposes. This form of interference with the individuals lives based on data collected for other purposes is referred to in this study as surveillance with non-purpose collected data. The most obvious example of such a situation is the case of the Data Retention Directive in the EU that will be discussed briefly below in section 2.3.2.2.

Technology that has a potential to be used for surveillance creates privacy concerns more directly than any other type of technology since it allows third parties to observe and watch over details from the private life of an individual that are intended to be private and not to be observed. Another discussion is the actual use of the devices for such purposes from law enforcement authorities, especially since it is also possible to observe and collect the same information from the individuals, with the use of different devices or systems of surveillance. Information on the location of an individual at a certain moment can be obtained, for example, from direct physical observation, the data of a GPS device, the mobile phone, the geo location of the computer IP when accessing internet, a RFID attached on the label of a shirt, by the data send by a smart energy meter, etc. Each of these methods and devices presents different levels of intrusion into the private sphere of the individuals. A human rights' based approach would suggest for the use of the surveillance measure which intrudes less with the private life of the individual.[46]

While the privacy concerns raised by advances in surveillance technologies are widely recognised,[47] recent technology developments have led to a convergence of these technologies with others not

[44] Vatney, M. (2006) The justifiability of state surveillance of internet communications as an e-security mechanism, available online at: http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/117_Paper.pdf (last check: 17.02.2015)

[45] Clarke, R. (1994) Dataveillance: Delivering '1984', in Green L., Guinery R. (eds.), *Framing Technology: Society, Choice and Change,* Allen & Unwin, available online at: www.anu.edu.au/people/Riger.Clarke/DV/PaperPopular.html (last check: 3.2.2015)

[46] The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, para. 25

[47] Kearns, T. (1999) Technology and the right to privacy: The convergence of surveillance and information privacy concerns, in *William & Mary Bill of Rights Journal*, vol. 7, no. 3, pp. 975-1011

designed for the purpose of surveillance. The existence of such devices and technologies challenges the classic understanding of surveillance and, in a way, blurs the distinction between the surveilled and the surveillor, between the State and private parties.[48] As a result, the protection of the right to privacy of European citizens presents new challenges. In the following sub-section, is analysed in how far surveillance with non-purpose built technology differs from traditional surveillance on the basis of a number of meta-dimensions.

2.2.1 Devices not built for the purpose of surveillance and their effect for the right to privacy

While the right to a protected private life in the EU is not an absolute one and there is the possibility for the State to interfere with it when fulfilling the legality requirements and meeting the set safeguards,[49] surveillance is *par excellence* a way in which the State interferes with the private life of the individuals. The proliferation of non-purpose built devices which enable the collection of personal information from individuals, extends the reach of the State and creates new risks for the safeguarding of the right to privacy.[50] For assessing if surveillance with devices not built for the purpose of surveillance meets the safeguards set for the protection of the right to privacy, it is first important to establish in how far this form of surveillance diverges from traditional surveillance.

Some authors have recognized the fact that the new and advanced technology has changed the way surveillance takes place. In a work of 2002, Gary Marx presents a comparison of 'new surveillance' - named in this way because of the advanced technology used that makes surveillance more a scrutinizing rather than an observing activity - with 'traditional surveillance' - that in his description is linked with physical surveillance and a scarce use of technology. This comparison is based on 26 dimensions of surveillance that he identifies.[51] According to Marx, development of technology has changed the way surveillance is performed at such a level as to fail the current dictionary definitions and understandings of the term. In comparison to traditional surveillance, new surveillance is considered in his work to be almost invisible, involuntary and integrated into routine activity, inexpensive, continuous, more intensive and more extensive.

The understanding of ´non-purpose built technology´ used for surveillance in this study does not entirely overlap with the concept of 'new surveillance' developed by Marx. This is the result of two reasons. The first reason is that Marx's definition of 'new surveillance' does not distinguish between surveillance technology and technology not built for the purpose of surveillance. The second reason

[48] For example, in the Concise Oxford Dictionary surveillance is defined as "*close observation, especially of a suspected person*"; for Marx, G.T. (2002) What's new about the "New Surveillance"? Classifying for change and continuity, in *Surveillance and Society*, vol. 1, no. 1, pp. 9-29, self-monitoring has emerged as an important theme, and is encouraged by the availability of a number of devices (as those that test for alcohol level, etc.) merging the lines between the surveilled and the surveillant

[49] See article 8(2) European Convention of Human Right and article 52 of the EU Charter of Fundamental Rights

[50] Mitsilegas, V. (2015) The transformation of privacy in the area of pre-emptive surveillance, *Tilburg Law Review*, vol. 20, pp. 35-57

[51] Marx, G. (2002) What is new about new surveillance?, *Surveillance and society*, vol. 1, no. 1, pp. 9-29, see table 1

is that the definition of surveillance with non-purpose built technology used in this study focuses on State activities while Marx's 'new surveillance' is extended also to purely private activities (as for example surveillance for commercial purposes) as well as to self-surveillance.

Also Marx's conceptualization of 'traditional surveillance' does not fully coincide with the understanding of traditional surveillance used in this study which includes into this category also all the surveillance performed via surveillance technology being this advanced or not. Despite this, the surveillance dimensions identified by Marx characterize the surveillance activity in general beyond any definition boundaries. That is the reason why his identified surveillance dimensions are used in this study for comparing and identifying any differences between traditional surveillance and surveillance with non-purpose built technology.

The comparison between traditional surveillance and surveillance with non-purpose built technology follows below. For making this comparison the 26 dimensions of surveillance identified by Marx have been grouped in four meta-dimensions of surveillance that correspond to the following questions: (1) who is the subject (active/passive) of surveillance;[52] (2) how is surveillance performed;[53] (3) what aspects of private life are interfered with;[54] and (4) when is surveillance taking place.[55] This grouping of the 26 surveillance dimensions reflects the legal aspects of surveillance for identifying the effects that surveillance with non-purpose built technology has for the right to privacy of the individuals. Each of the meta-dimensions is discussed in turn.

(1) Who is the subject of surveillance?

When assessing the subject of surveillance one has to discuss both its sides. Below it is first discussed the active subject of surveillance, the surveillant, and subsequently the passive subject, the surveilled.

a) The active subject of surveillance

In traditional surveillance, the surveillant is represented by the State and its authorities. Private parties play a role in this State activity in specific and clearly defined cases, under clear authorization that is in conformity with all the set safeguards (as for example when private parties are authorized

[52] Under this question are grouped the surveillance dimensions of: consent, data collector, availability of technology, object of data collection, ratio of self to surveillant knowledge, identifiability of object of surveillance, emphasis on and who collects the data

[53] Under this question are grouped the surveillance dimensions of: senses, visibility, cost, location of data collector/analysers, ethos, integration, data resides, comprehensiveness, realism, data analyses, data merging, data communication

[54] Under this question are grouped the surveillance dimensions of: context, depth and breadth

[55] Under this question are grouped the surveillance dimensions of: timing, time period and data availability

to install a CCTV for the scope of protecting their premises).[56] The centralization of surveillance in the hands of the State is mirrored in the exercised control on surveillance as well as in the performance under clear conditions and safeguards.

Due to the technology development and especially due to the existence of devices that are non-purpose built for surveillance but that have the ability to perform this task, the person of the surveillant cannot be linked anymore exclusively to the State. Devices that might serve for surveillance are available in the hands of the citizens and, as it was seen in different examples, most of personal data collected with the help of technology are nowadays available with service providers. As a result, the role of private parties becomes more prominent.

Because of the ability and the spread of technology it is possible for State surveillance to be performed on a generalized and massive scale without the need to target previously identified individuals. Furthermore, the individuals can themselves collaborate in their own surveillance blurring in this way the distinction between the active and passive subject of such activity. The grey area in which it is difficult to distinguish between the active and the passive subject of surveillance is created not only because individuals carry with them devices that have a potential to be used for surveillance, but also because they use and feed with data a number of devices/softwares to organize their activities and even to monitor themselves (as for example keeping online agendas or using an e-health application in smart phones).[57]

b) The passive subject of surveillance

The comparison between traditional surveillance and surveillance with non-purpose built technology has relevance also for the passive subject of surveillance. Traditional surveillance is normally performed towards individuals for whom there is a surveillance mandate. It is quite expensive and inefficient to surveil other individuals in the absence of individual mandates, though exceptions to such a rule would come from non-democratic regimes. For traditional surveillance, in general, mass surveillance of individuals is restricted to clear and precise public spaces as for example the access in airports or being in certain CCTV covered areas. In situations in which non-targeted individuals are incidentally surveilled, it is easy to distinguish them from the targeted subject of surveillance (as for example when incidentally intercepting the phone call of a third person having access to the wiretapped device).

[56] Case C-212/13 Ryneš EU:C:2014:2428

[57] Kang, J., Shilton, K., Estrin, D., Burke, J., Hansen, M. (2012) Self-surveillance privacy, in *Iowa Law Review,* vol. 97, pp. 809-847

Surveillance with non-purpose built technology creates more possibilities for situations of mass surveillance and incidental surveillance. The introduction of pre-emptive surveillance[58] that aims to detect all situations that might have or not any future relation to a possible future criminal activity together with the technology capabilities has increased the use of mass surveillance. This is now not linked anymore with the presence of the citizen in certain spaces but with the use of certain technology. Technology creates the possibility that one might be surveilled not only when being in well-defined public spaces, but also when being in the intimacy of his own private space. In addition, it is more difficult to distinguish the cases of incidental surveillance. When analysing data that have been collected and retained from the use of a device, it is difficult to be certain that the device was used by one person or another (for example another member of his household in cases of smart meters). Even if surveillance with non-purpose built technology presents itself as more intrusive than traditional surveillance,[59] incidental involvement of third persons might make this less accurate both in the cases of individual surveillance and in the cases of mass surveillance.

(2) How is the surveillance performed?

Surveillance is generally performed in two ways. Either by directly observing the activities of the individual (direct surveillance) or by observing the trace of data that one leaves behind (dataveillance). The way surveillance is performed is different in cases of traditional surveillance and in cases of surveillance with non-purpose built devices.

Traditional surveillance is mainly direct and surveillance devices, even the advanced ones, need an activation from the surveillor (as for example when installing a bug or using a terahertz body scanner). Dataveillance[60] is part of traditional surveillance only in specific cases and closely linked with the surveillance technology used (as for example when tracing a CCTV footage).

Surveillance with non-purpose built technology is folded into routine activity and based more on the data collection and retention capability of the devices, therefore has mainly the form of dataveillance. This form of surveillance (due to the possibility of other parties to access the devices used for surveillance) might create the risk that incorrect or unreliable data are used and processed.[61] Devices and the programmes installed in them would collect data for default and these data, even if not collected for the purpose of surveillance might be further used for this purpose. Surveillance with non-purpose built technology is however not limited to dataveillance. It allows also

[58] Brakel, R., van, De Hert, P. (2011) Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Cahiers Politiestudies*, vol. 3, no. 20, pp. 163-192

[59] Marx, G. (2002) What is new about new surveillance? Classifying for change and continuity, in *Surveillance and Society*, vol. 1, no. 1, pp. 9-29

[60] For a definition of dataveillance see Clarke, R. (1994) Dataveillance: Delivering '1984', in Green L., Guinery R. (eds.), *Framing Technology: Society, Choice and Change,* Allen & Unwin, available online at: www.anu.edu.au/people/Riger.Clarke/DV/PaperPopular.html (last check: 3.2.2015)

[61] Chandler, J. (2009) Privacy Versus National Security: Clarifying the Trade-off, in Kerr, I., Lucock, C., Steeves V. (eds.), *Lessons from the Identity Trail: Privacy, Anonymity and Identity in a Networked Society*, pp. 121-138

for direct observation as for example when remotely activating devices and using them for surveillance purposes (as in the case of activating the microphone of a mobile phone and using it as a portable bug), or when connecting to the satellite to access the location of the GPS navigation system of a car, or even when receiving data in short time slots from smart electricity meters.

(3) What aspects of private life are interfered with?

The private sphere of the individuals consists of a number of aspects that have been identified earlier by Clarke (2006)[62] and further elaborated by other authors.[63] These include: (i) privacy of the person concerned with the privacy of an individual's body, (ii) privacy of personal behaviour,[64] (iii) privacy of personal communication, (iv) privacy of personal data,[65] (v) privacy of location and space, (vi) privacy of thoughts and feelings,[66] and (vii) privacy of association. The aspects of privacy that might be interfered by surveillance as well as the separation of subcategories have increased due to the development of technology. For example, the privacy of the thoughts and feelings could not be easily interfered with the traditional ways of surveillance but it is possible now due to the new technology with devices not built for the purpose of surveillance.

Also the level of intrusion into each aspect of privacy diverges in cases of traditional surveillance and surveillance with non-purpose built technology. For example, placing a bug inside the home for listening to the conversations of an individual is intrusive, but remotely activating the microphone of a mobile phone and using it for the same purpose is even more so. Someone would carry a mobile phone with himself in most places and therefore be vulnerable to the infringement of the privacy of communications almost everywhere and with everyone. The same would be when physically following someone on the streets or installing a GPS device in his car, or receiving the same information from the mobile phone GPS. Again, in the latter case the coverage and the level of intrusion would be more intensive. Surveilling via the data collected by a smart meter, on the other side, might work as having a continuous physical presence inside a house that detects in real time (or quasi) many activities taking place therein. From the above examples, it is clear that surveillance with non-purpose built technology, because of the nature and the way non-surveillance technologies in the hands of the individuals are used, presents itself as having a higher level of intrusiveness into the

[62] Clarke, R. (2006) What's 'Privacy'?, available online at: http://www.rogerclarke.com/DV/Privacy.html (last check: 10.07.2013)

[63] Wright, D., Raab, C. (2014) Privacy principles, risks and harms, *International review of law, computes and technology*, vol. 28, no. 3, pp. 277-298

[64] Kalogridis, G., Denic, S.Z. (2011) Data mining and privacy of personal behavior types in smart grid, in *IEEE*, pp. 636-642

[65] The difference and interlink between privacy and data protection are discussed in chapter 3 of this study

[66] See for example the newest developments on wireless brain–computer interface in Borton, D.A. et al. (2013) An implantable wireless neural interface for recording cortical circuit dynamics in moving primates, *Journal of Neural Engineering*, vol. 10, no. 2, pp. 16; Young, S. (2013) A wireless brain-computer interface, available online in: http://www.technologyreview.com/news/512161/a-wireless-brain-computer-interface/ (last check on 24.04.2013)

private life of the individuals than traditional surveillance.[67] The examples mentioned above are explained in a more detailed fashion in the case studies of chapter 4.

(4) When does surveillance take place?

Traditional surveillance is mainly taking place simultaneously, at the moment, though the technology used might give possibilities for time-shifting the actual checking of the information. Surveillance with non-purpose built devices creates the possibility to also bring the past into the present and even to predict the future. Retention of personal data by devices and services one uses, for example, creates the possibility to look back at the past behaviour and activities of an individual. As a result, there is the possibility for retroactive surveillance - to check the past activities of an individual at a time he was not suspected as related to any criminal activity. It does not go without saying, however that this possibility of surveillance on the bases of retrieving retained data might lead to infringements of other rights of the individuals, as for example their right to a due process and the presumption of innocence. Data mining and analyses might on the other side give the possibility for future predictions on the behaviour of individuals and serve for fulfilling the scope of pre-emptive surveillance.

There is a difference also in the timing of surveillance. While traditional surveillance mainly takes place at single or intermittent points of time, surveillance with non-purpose built technology is embedded in routine activities and can be continuous and omnipresent. Also the speed of the availability of the results of surveillance might present certain time lags for traditional surveillance (especially when dealing with physical surveillance and in the lack of technology) while it is available in real time for surveillance with non-purpose built technology. The differences between traditional surveillance and surveillance with non-purpose built technology on the basis of the identified meta-dimensions of surveillance are summarised below in Table 1.

From the comparison, it is clear that the two forms of surveillance are different from each other and that surveillance with non-purpose built technology is more intrusive into the life of the individuals than traditional surveillance. Surveillance with non-purpose built technology might create an easy extension of mass surveillance situations, as it is the case with using non-purpose collected data for surveillance. Due to the use of technology it also includes the possibility for incidental surveillance of untargeted individuals as an integral part of itself. In addition, the possibility for retroactive surveillance creates situations of interference with the life of individuals at a time that they were not qualifying as subjects of surveillance.

[67] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, Opinion of AG Cruz Villalon, para. 74

Table 1

Surveillance / Meta dimension	Traditional	With non-purpose built technology
Active subject	the State authorised private parties	the State private parties self-surveillance
Passive subject	targeted individual untargeted individuals in clear situations (mass surveillance) incidental surveillance	targeted individual untargeted individuals using certain technologies (mass surveillance) more incidental surveillance
Way of surveillance	direct (mainly but also) dataveillance	dataveillance (mainly but also) direct
Private life aspects	privacy of the person privacy of behaviour privacy of communication privacy of personal data privacy of location and space privacy of association privacy of thoughts and feelings	privacy of the person privacy of behaviour privacy of communication privacy of personal data privacy of location and space privacy of association privacy of thoughts and feelings
Time of surveillance	present past	past present future

2.2.2 Concluding remarks

The aim of this section was to define surveillance with non-purpose built technology and to highlight the differences with traditional surveillance for assessing the effects that they have when interfering with the right to privacy of individuals. Non-purpose built technology used for surveillance does not only have an effect on the quantity and quality of the data collected. It also has an effect on the way surveillance is conducted and it creates new challenges for safeguarding the right to privacy of the individuals.

With regards to the active subject of surveillance, in cases of surveillance with non-purpose built technology the role of private parties, being these service providers or other individuals, increases. In addition, surveillance with non-purpose built technology extends more often the interference with the private life of untargeted individuals either in the form of mass surveillance or increasing the possibilities for incidental surveillance.

Surveillance with non-purpose built technology is mainly performed as dataveillance, accessing non-purpose collected data but it gives the possibility also for direct surveillance via remote access to the devices and benefiting of their surveillance abilities. It increases the aspects of the private life of the individuals that can be interfered with as well as the level of interference. At the same time, it creates the possibility not only for a continuous surveillance but also for reviving the past activities and even for predicting the future behaviour of the individuals.

The choice on traditional surveillance or surveillance with non-purpose built technology is of course left with the national authorities responsible for the prevention, investigation, detection and prosecution of criminal activities on the basis of the safeguards offered by the laws and the proportionality principle. A human rights' based approach, though, would advise for the use of traditional surveillance when the same information can be obtained.

2.3 Challenges to the right to privacy

The previous section identified a number of legal challenges to the right to privacy that surveillance with non-purpose built technology presents. These challenges are: (1) the increased risk for incidental surveillance, (2) the facility for engaging in mass surveillance and, (3) the possibility for retroactive surveillance. In the following sub-sections (2.3.1, 2.3.2 and 2.3.3 respectively) each of these challenges is addressed separately and the way in which they are addressed so far in the European legal framework is analysed. This allows to assess if the legal framework that is constructed in light of traditional surveillance is adequately safeguarding the rights of the individuals also in situations of surveillance with non-purpose built technology. Detailed concluding remarks are presented at the end of each sub-section.

2.3.1 Incidental surveillance

As argued in the previous section, among other challenges, surveillance with non-purpose built technology leads to more possibilities of incidental surveillance for untargeted citizens, threatening their right to a protected private life. The aim of this sub-section is to assess the way in which incidental surveillance is dealt with thus far at European Union level and the existing safeguards for the protection of the rights of the individuals in such situations. For doing this, incidental surveillance is first defined and then the way the Courts have dealt with it thus far is assessed. Since there have not yet been any cases on incidental surveillance discussed at the Court of Justice of the EU (CJEU), the focus will be on a number of decisions from the European Court of Human Rights (ECtHR) where situations of incidental surveillance have been discussed in two instances: (1) when the information obtained by means of incidental surveillance has an interest for the law enforcement authorities, and (2) when the information does not have an interest for law enforcement authorities.

There is not a harmonized approach of incidental surveillance or of its definition in Europe. In UK, for example, is referred to as "collateral intrusion".[68] In another work, incidental surveillance is referred to as "surplus information" or a by-product of information that is collected with an authorization, but

[68] See Guiding document to the UK Regulation of Investigatory Powers Acts 2000, the Leeds City Council Legal Services which defines "collateral intrusion" as interference with the privacy of persons, other than the subject of the surveillance, available online at:
http://www.leeds.gov.uk/docs/RIPA%20Guidance%20and%20Procedure%20-%20May%202013.pdf (last accessed: 30.03.2015)

that is not covered by that same authorisation.[69] In this study incidental surveillance is defined as the accidental collection of data on individuals that are not the target of the surveillance activity and mandate.

Independent from the definition, incidental surveillance might have the effect of interfering with the private life of individuals that are not the target of a surveillance measure. The life of the individuals is captured, as its denomination describes it, incidentally. In cases of non-State surveillance, the most prominent examples of such incidental interference with the life of others would be when, for example, informing via social media the location of a friend (e.g. "… drinking with X a coffee at Y bar in Z city …").[70]

State surveillance with non-purpose built technology creates more possibilities for individuals to be incidentally surveilled and this is, may be, an unavoidable consequence of surveillance. Such surveillance is not limited only to location technologies.[71] Smart meters would, for example, show the usage of electricity for all the members of the household. Mobile telephony devices are easily transferred, lost or stolen, and electronic communication accounts are often left active. Communications of individuals may therefore be incidentally intercepted because they are using a third party intercepted device or account. To be incidentally involved in a situation of surveillance does not mean however that such individuals do not have a right of protection for their privacy.

The following analyses takes a critical approach to the application and interpretation of the right to privacy by the ECtHR in situations of incidental surveillance. Though the legal framework applicable to the right to privacy and to surveillance in the European Union is explained in detail in chapter 3, the sub-section discusses the applicable legal framework only to the limited scope of incidental surveillance. The analysis shows the shortcomings of the application of the laws and explores its limits in light of technological advances. It is argued that in the area of incidental surveillance the ECtHR has failed in its mission to protect the right to privacy of the incidentally involved individuals. The example of incidental interception of communications is used for making the analyses more tangible.

[69] See Nowak, K. (2011) Vetting surplus information before it can lead to human right infringements, deliverable prepared for DETECTOR (Detection technologies, terrorism, ethics and human rights) FP7 project, available online at: http://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCgQFjAB&url=http%3A%2F%2Fwww.detecter.bham.ac.uk%2Fpdfs%2FD15.2_Vetting_Surplus_Information.doc&ei=gdtdVdi0FcG4UYbQgLgN&usg=AFQjCNEqL-D2U6fiHzZ5wUZ1iIsK2R9axQ&bvm=bv.93756505,d.d24 (last accessed: 21.5.2015)

[70] Leaver, T., Lloyd, C. (2015) Seeking transparency in locative media, in Wilken, R., Goggin, G. (eds.), *Locative media*, pp. 162-176

[71] De Souza e Silva, A., Gordon, E. (2014) Net locality, in Adey, P., Bissell, D., Hannam, K., Merriman, P., Sheller, M. (eds.), *The Routledge Handbook of Mobilities*, pp. 134-142

2.3.1.1 Incidental interception of communications

With the creation of new ways of communication, also the possibility for being incidentally intercepted has increased. The use for communication of mobile devices as well as of internet accounts, has increased the possibility for individuals to make use of third party devices or accounts for which there is a surveillance mandate. Being involved incidentally in a surveillance situation does not erase, however, the right to privacy of the individual as well as the interest to know how their personal data is used.

A communication needs by definition at least two parties: a sender of the information and a recipient of it. As such, being part of a communication which is intercepted does not make the authorized interception become automatically unlawful in respect to the targeted interlocutor.[72] This is different, however, from the situation of someone whose communication is being incidentally intercepted because he is using a device or account for which there is a surveillance mandate without being himself the target of such a measure. These are the situations of incidental surveillance discussed in this sub-section.

The interception of communications discussed in this sub-section is related with cases of targeted State surveillance. Even though every person that uses the intercepted device or account might be incidentally intercepted, because of the limited range of surveillance such situations are not considered as falling under mass surveillance. The same approach is confirmed in the *Lambert* case where the ECtHR stated that a very large number of people will be deprived of the protection of the law, namely all those who have conversations on a telephone line other than their own, if they are not allowed to challenge the intercepting mandate that was issued for the targeted individual as their own.[73] As a result the incidentally involved individual has to challenge the validity of the surveillance mandate as if it was directed to him and is not required to challenge the necessity of the laws that introduce surveillance, as it would have been the case in situations of mass surveillance.[74]

In the following sub-sections, incidental interception of communications is discussed for situations in which the interception has an interest for the law enforcement authorities (sub-section 2.3.1.1.1) and situations that do not have an interest for the law enforcement authorities (sub-section 2.3.1.1.2). For being able to assess how the right to privacy of the individuals is addressed in such situations, attention is payed to ECtHR decisions in situations of incidental surveillance. The applicable legislation, discussed in detail in chapter 3, is discussed in these sub-sections to the extend needed for understanding in how far situations of incidental surveillance are already regulated.

[72] Drakšas v. Lithuania, ECHR application no. 36662/04, 31 July 2012, para. 57
[73] Lambert v. France, ECHR application no. 23618/94, 24 August 1998, para. 38
[74] Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 4

2.3.1.1.1 Incidental interception of communications that have an interest for the authorities

For the purposes of this sub-section 'incidental interception of communications' means the listening or recording of communications of an individual that is not the direct subject of the intercepting mandate. For example: there is reasonable suspicion that person A has been collaborating for committing crime X. There is a mandate for tapping the phone of A in order to collect valuable information that will help the authorities for solving case X. B uses the phone of A and in his conversation with a third person gives relevant information on crime Y. In this situation, the intercepting authorities have collected incriminating information on person B in relation to crime Y - an investigation for which they did not have a mandate.

When applying the provision of article 8 ECHR on the protection of the private life[75] to such a situation it is clear that there has been an interference of the public authorities with the private life and correspondence of an individual (B) by recording his communication with a third party. The interference was incidental, therefore without a surveillance mandate or any running investigation for him. Such an interference falls under article 8(1) ECHR and, since it was incidental, it cannot be justified under the second paragraph of the article.[76] Since the recording of the communication of person B, was not done on the basis of a personal mandate or for the investigation of crime Y, it is not necessary to consider if the other elements of the article are fulfilled. Furthermore, no individual assessment was undertaken for evaluating if the interference in such a case was necessary and proportionate in a democratic society.

It is therefore quite surprising to follow the argumentation of the European Court of Human Rights in the *Kruslin* case (very similar with the example above of incidental interception of communications) where the incidental recording of a phone conversation was the decisive piece of evidence the judge relied upon in the proceedings against the applicant.[77] In applying the test contained in article 8 ECHR, the ECtHR found that there was an interference with the right to correspondence and to private life of the applicant. For the ECtHR, however, the interference was in accordance with the national laws, as interpreted and applied by the national authorities. The ECtHR attention was on the original intercepting mandate (the one for person A – or in the *Kruslin* case for Mr. Terrieux). Since the French law was not detailed on this point, the ECtHR´s elaboration focuses on the definition of the applicable law. It is clarified that under the term "applicable law" are included also unwritten laws and judicial decisions.[78] But while this is true and stands for the tapping of the phone line and the interception of the communications of Mr. Terrieux, the fact remains that the tapping mandate was not permitting an interference with the private life of Mr. Kruslin.

[75] For an extensive analyses of article 8 ECHR please see Chapter 3, section 3.2
[76] M.M. v. The Netherlands, ECHR application no. 39339/98, 8 April 2003, para. 45
[77] Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 9
[78] Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 28

For the ECtHR, the identification of the relevant laws and their interpretation falls within the competence of the national authorities. The quality of the law is, however, assessed by the ECtHR.[79] In extending the meaning of "law" also to unwritten laws, the ECtHR accepts the argument that it was an established practice for the judges to issue mandates for tapping phones as well as for making use in one case of relevant evidence from another case.[80] Tapping practices existed in France from the nineteenth century and were recognized by the case law. Giving the main attention to such an issue, the ECtHR seems to forget the fact that the interference with the private life and the correspondence of the applicant was, in *Kruslin*, done incidentally. What the ECtHR is assessing and justifying in the judgment is the use of evidence in a process while not considering the way this was obtained.[81] Even if the tapping of the phone line was done in accordance with the law, the interference with the private life of Mr. Kruslin was not because the guarantees of article 8 ECHR were not taken into account in his case.

Article 8 ECHR has the effect of ensuring that police conduct meets certain minimum standards. If the use of evidence obtained in breach of this provision is not similarly regulated, the standards set for policing action will only have a theoretical importance.[82] With this line of argumentation the ECtHR fails to protect the private life and correspondence of individuals in incidental surveillance situations. It is to be noted that the wording of the ECtHR in the *Kruslin* case is identical to the one in *Huvig*,[83] which was decided on the same day. Also in that case the main focus was on defining the notion of "applicable law".[84] With this approach the ECtHR leaves undiscussed the incidental surveillance element and fails to address the problems that these create for the protection of the right to privacy of individuals that find themselves in such a situation.

Even if in the end in *Kruslin* the ECtHR decided that there had been a violation of article 8 ECHR since the French law on wiretapping, in general, did not offer adequate safeguards for the surveilled individuals, the decision is very important because it considers incidental interceptions as being in accordance with the law. With its reasoning, the ECtHR implicitly allows the extension of an intercepting mandate for the communications of an individual, to all other persons making use of the same tapped device or account. In other words, this line of argumentation opens *de facto* the doors for public authorities to interfere with the private life and the correspondence of all persons having access to a taped phone, even if they themselves are not under any investigation and without any prior assessment of the facts of the case. If not given the needed attention this line of interpretation of the law might take the dimensions of mass surveillance of persons having access to a certain device or account.

[79] Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 29
[80] Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 19
[81] Vervaele, J.A.E. (2005) Terrorism and information sharing, *Utrecht Law Review*, vol. 1, no. 1, pp. 1-27
[82] Taylor, N. (2003), Policing, privacy and proportionality, *European Human Rights Law Review*, Supplement (Special issue: privacy 2003), p. 86
[83] Huvig v. France, ECHR application no. 11105/84, 24 April 1990
[84] Tomilson, E.A. (1993), The saga of wiretapping in France: What it tells us about the French criminal justice system, *Louisiana Law Review*, vol. 53, No. 4, p. 1133

A similar situation was discussed in *Lambert* where the European Court of Human Rights focused on the legal safeguards and made "effective control" available for incidentally surveilled individuals.[85] Since, as the result of its reasoning, all persons having a conversation on a tapped third party telephone line are deprived of the protection of the law,[86] the ECtHR gives the incidentally involved individuals the possibility to challenge the validity of the tapping mandate as if they were in person addressed by it.

What the ECtHR is doing in such a situation is to extend *ex post* the original mandate issued for person A also to the incidentally tapped person B, giving to the latter the legal possibility to challenge the validity of the tapping mandate in front of national courts. The same line of argumentation was followed also in *Matheron.*[87]

The possibility for "effective protection" is an *ex post* adjustment and improves only partially the situation of the incidentally surveilled person. In issuing the surveillance mandate the authorities have not considered the need of such an interference in his situation and therefore it would be difficult to successfully challenge the mandate on its merits.

The interpretation and application that the European Court of Human Rights is giving to the provision of article 8 ECHR is therefore failing its purpose of protecting the right to privacy of the individuals in the cases of incidental surveillance. The ECtHR reasoning is bypassing the fact that for taking a decision on the application of surveillance measures for a concrete case, the authorities must evaluate its characteristics and decide on the adequate investigatory measures on the basis of the necessity and proportionality principle. This contrasts also to the fact that the ECtHR considers in general audio and video intercepting measures as very intrusive and suggests the application of stringent criteria in deciding on their use in compliance with the proportionality principle.[88]

The way in which the law is applied in such situations creates double standards. The minimum requirements of article 8 ECHR are strictly checked in the case of an individual surveillance mandate but are neither taken into account nor guaranteed for individuals that find themselves incidentally in a situation of interference with their private life. The right to privacy of individuals whose private lives are incidentally surveilled in the cases in which the surveillance results turn to have a relevance for law enforcement authorities, is therefore not guaranteed.

[85] Lambert v. France, ECHR application no. 23618/94, 24 August 1998, para. 40
[86] Lambert v. France, ECHR application no. 23618/94, 24 August 1998, para. 38
[87] Matheron v. France, ECHR application no. 57752/00, 29 March 2005, para. 43
[88] Uzun v. Germany, ECHR application no. 35623/05, 2 September 2010, para. 68-69; see also Wicker, S.B. (2011) Cellular telephony and the question of privacy, *Communications of the ACM*, vol. 54, no. 7, p. 88

2.3.1.1.2 Incidental interception of communications that do not have an interest for the authorities

As already discussed in the previous sub-section, incidental surveillance of individuals is considered by the European Court of Human Rights as lawful interference with the private life of the individuals when the information obtained has relevance for the law enforcement authorities. Even if such an approach conflicts with the right to protection of privacy, it has to be kept in mind that the ECtHR has to strike a balance between this right and the societal interest for national security, public safety, and prevention of disorder or crime. This sub-section discusses the situation of incidentally intercepted communications of individuals when the obtained information does not have any value for the authorities in terms of prevention, investigation, detection and prosecution of crimes.

In general, for the European Court of Human Rights, the mere collecting and storing of personal data from individuals, despite the fact that the data has not been subsequently used, amounts to an interference with their private life as established in paragraph 1 of article 8 ECHR.[89] Incidentally collected data must be considered in the same way. Since in cases that do not have any value for crime control, there are no other interests to balance to the right to protection of privacy, these data must be deleted.

If the data have not been deleted, Recommendation R87(15) of the Council of Europe recommends the Member States to inform the person whose data have been collected by police authorities, once these do not have any more an effect for the specific investigation.[90] Such *ex post* notification has a specific importance for the protection of individuals in cases of incidental recording of data since it is an essential safeguard against abuse of monitoring powers and it is an important part of the right to an effective remedy before the national courts. This important Recommendation does not have, however, any binding effect, and has not been incorporated so far in most of the national legislation of the Member States.[91] As of May 2018, with the entry into force of Directive 680/2016,[92] the individuals will have the right to be informed, but as it is discussed in Chapter 3, sub-section 3.6.2.1, this has to be done on the request of the individual himself – whom in most of the cases does not have a reason to suspect of having been surveilled.

[89] Leander v. Sweden, ECHR application no. 9248/81, 26 March 1987, para. 48; Kopp v. Switzerland, ECHR application no. 23224/94, 25 March 1998, para. 53, Amann v. Switzerland, ECHR application no. 27798/95, 16 February, para. 69

[90] Recommendation R87(15) of the Council of Europe, principle 2.2. In general, on the problems following the non-binding nature of R87(15) see Study on Recommendation No. R(87)15 of 17 September 1989 regulating the use of personal data in the police sector – 'Data Protection Vision 2020: Options for improving European policy and legislation during 2010-2020' by Joseph A. Cannataci, available online at: http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf (last accessed: 20.2.2015)

[91] De Hert, P., Boehm, F. (2012) The rights of notification after surveillance is over: Ready for recognition?, in Bus et al. (eds.), *Digital enlightment year book 2012*, IOS Press, p. 19

[92] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89–131

The European Court of Human Rights has applied this 'notification' principle in a number of cases.[93] The most significant decision is *Ekimdzhiev* were the ECtHR clearly established that omission of notification of surveillance measures, once it does not risk to jeopardize the inquiry, amounts to violation of article 8 ECHR.[94] In the doctrinal debate, some authors applaud the decision of the ECtHR in *Ekimdzhiev* and support the introduction of such a principle also at EU level.[95] Other authors are however sceptic,[96] since they are sensitive to the negative impact that an *ex post* notification might have for the reputation of the person who was the target of the surveillance measure.

Despite the doctrinal debate, the use of *ex post* notification of surveillance measures has special importance in cases of incidental surveillance since there is no other possibility to know and challenge this surveillance in case they would not arrive before the national courts. For these cases *ex post* notification would serve as an essential safeguard against abuse of monitoring powers and as an important part of the right to an effective remedy.

2.3.1.2 Concluding remarks

The aim of this sub-section was to analyse how the right to privacy of individuals that find themselves in situations of incidental surveillance is protected thus far in the EU. As it was already seen in the previous section, the increase of situations of incidental surveillance is one of the challenges to the right to privacy that surveillance with non-purpose built technology creates. In this sub-section it was argued that individuals enjoy less protection of their right to privacy in cases of incidental surveillance than in those of targeted surveillance.

Secret surveillance measures, especially when applied pre-emptively or to an unidentified number of persons, create a situation in which the State distrusts its own citizens. According to some authors, these must be substituted by trust and consent.[97] But being aware of being surveilled is considered

[93] Klass v. Germany, ECHR application no. 5029/71, 6 September 1978, para. 50; Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 114

[94] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, ECHR application no. 62540/00, 28 June 2007, para. 91

[95] De Hert, P., Boehm, F. (2012) The rights of notification after surveillance is over: Ready for recognition?, in Bus et al. (eds.), *Digital enlightment year book 2012*, IOS Press, p. 19; Boehm, F., De Hert, P. (2012), Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law, *European Journal of Law and Technology*, vol. 3, no.3

[96] Alonso Blas, D. (2010) Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom, *ERA Forum*, vol. 11, pp. 233-250

[97] Norris, C., Murakami Wood, D. (2009) Evidence, in House of Lords, Selected Committee on the Constitution, Surveillance: Citizens and the State, HL paper 18-II, second report of session 2008-2009, Volume II: Evidence, p. 26

ineffective in cases of prevention, investigation, detection and punishment of crime.[98] The scope of the protection of the right to privacy of individuals marks the introduction of minimum safeguards in those cases in which there is a legitimate need that justifies the interference with their private life. These safeguards are designed to prevent abuse from the public authority in cases of interferences with the private sphere of the individuals. The way the ECtHR has applied these safeguards in cases of incidental surveillance fails this purpose.

In targeted surveillance cases, the protection of the rights of individuals whose communications are incidentally intercepted, is not very strong. In these cases, the risk is created that the interception of communication on the basis of a valid mandate for one person, is extended to everyone using the same tapped device or account, independent of the relation with the investigated or the investigation. As a result, a situation of surveillance of categories of individuals identified only on the access that they have to a certain device is created. The possibility for these persons to challenge the validity of the intercepting mandate protects them only partially, since the mandate was not tailored to their case and no personal evaluation has been considered at the moment the intercepting mandate was issued.

The *ex post* notification of surveillance measures would play an important role in cases of incidental surveillance of individuals, especially if the data collected does not have any relevance for the prevention, investigation, detection and prosecution of crimes. This is a minimum requirement to enable legal protection of individuals in a democratic society. Such notification would give the possibility to the individuals to ask the protection of their rights before the national courts in cases of abuse.

It is not up to this author to speculate as to whether the authorities must hang up or stop recording once they realize that another person is being incidentally intercepted. It is true, as already discussed above, that protection of privacy is not an absolute right but it has to be counterbalanced by other societal interests. But incidental interception of communications, as interpreted and applied by the ECtHR, does not comply with the minimum safeguards of article 8 ECHR which require the *ex ante* evaluation of the necessity of the surveillance measure. It must therefore be considered as an infringement of the protection offered by the article and the information obtained incidentally should be deleted. Another option, in light of the balancing of different interests' discussion, is to consider the information collected incidentally as an indication that gives the authority the possibility to start an investigation on the individual, but not to consider it as lawfully collected evidence. The different approach that the Member States have in this respect[99] calls for a harmonized regulation of

[98] Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para.135-136, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, ECHR application no. 62540/00, 28 June 2007, para. 90

[99] For the different approach of the Member States the DETECTER FP7 project refers to: Danish Procedural Code, Chapter 71, 780-791 b §§; Finish Compulsory Measures Law, Chapter 5a (450/87); Dutch Wet Bijzondere opsporingsbevoegdheden, art. 126 cc-dd; German Strafprozessordnung, 98, 100, 110, 163 §§; the Spanish doctrine of "descubrimientos ocasionales o casuals"

the way to deal with incidental surveillance at European Union level for the proper protection of the right to privacy in all situations.

With the development of technology and the possibility to use for surveillance devices that are not built for this purpose, law enforcement authorities will face more situations of incidental surveillance. It is therefore not anymore possible for the European Courts to ignore the situations of incidental surveillance and it is necessary for the European Court of Human Rights to revise its line of argumentation in order to offer full application of the provision of article 8 ECHR, in all situations. The potential of technology for incidentally interfering with the life of untargeted individuals and the effect this has for their right to a protected private life must be taken into account when deciding on the use of a device for surveillance purposes.

2.3.2 Mass surveillance and non-purpose collected data

Devices that have an ability to be used for surveillance even if not built for that purpose increase the possibilities for mass surveillance of European citizens. This sub-section takes a normative approach in analysing the effects of mass surveillance for the right to privacy of the individuals and the way this form of surveillance is addressed thus far in EU law.

Even if innocent, and not related with any criminal activities, there are chances that we are watched by the State(s) every time we use internet, make a phone call or send an e-mail.[100] Other devices that we are asked to use in our households, as for example smart energy meters,[101] open the possibility for being watched also when turning on a light, starting the oven, or changing the television channels.[102] In the logic of mass surveillance programmes we can all potentially be, sooner or later, involved in some criminal activities; we are all therefore suspects. It is needless to say that the

[100] Greenwald, G., MacAskill, E., Poitras, L. (2013) Edward Snowden: the whistleblower behind the NSA surveillance revelations, *The Guardian* (9 June 2013), available online at: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (last accessed 20.1.2014); MacAskill, E., Borger, J., Hopkins, N., Davies, N., Ball, J. (2013) GCHQ taps fiber-optic cables for secret access to world's communications, *The Guardian* (21 June 2013), available online at: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (last accessed 20.1.2014)

[101] Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, OJ L 211, pp. 94-136, article 3(8)

[102] Mills, E. (2012) Researchers find smart meters could reveal favorite TV shows, *CNet News* (24 January 2012), available online at: http://news.cnet.com/8301-27080_3-57364883-245/researchers-find-smart-meters-could-reveal-favorite-tv-shows/, (last accessed 27.4.2013); Greveler, U., Justus, B., Loehr, D., (2011) Multimedia Content Identification Through Smart Meter Power Usage Profiles, available online at: http://epic.org/privacy/smartgrid/smart_meter.pdf (last accessed 27.4.2013); Cuijpers, C., Koops, B.-J. (2013) Smart metering and privacy in Europe: Lessons from the Dutch case, in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds.), *European data protection: Coming of age*, Springer, pp. 269-293

increase in the use of mass surveillance is closely linked with the development of technology.[103] Devices that we use in our daily lives, even if not originally built for the purpose of surveillance, offer possibilities for cheap and expedient mass collection of personal information and data (dataveillance) as well as for direct surveillance. As already seen in section 2.2 of this chapter, also the use for surveillance of data collected for other purposes falls under the definition of surveillance with non-purpose built technology used in this study.

The shift of our society to a pre-crime one can also affect some persons' relationships to others and to the State, in the sense of introducing a "culture of suspicion" which affects mutual trust, social inclusion and even creates a vague form of presumption of guilt.[104] This context of fear and distrust is what has sometimes been described as the "chilling effect" of the surveillance society,[105] which can seriously affect individuals' exercising of their rights.

Mass surveillance programmes have been discussed in the literature in the light of the problems that they create for the right to a protected private life of the individuals and the principle of proportionality.[106] Their extensive use by intelligence services and law enforcement authorities has also raised the question whether these programmes can be justified in a "security weighs more than other individuals' fundamental rights" approach - in reality questioning the very fundamentals of a democratic society.[107] After this introduction, mass surveillance practices used in the EU are discussed in light of the case law from the ECtHR (sub-section 2.3.2.1). Than the data retention from electronic communications in the EU (which qualifies as a specific case of mass surveillance) is discussed together with the safeguards that the CJEU set for such cases (sub-section 2.3.2.2). The challenges that mass surveillance presents for the right to privacy of European citizens are summarized in the concluding remarks (sub-section 2.3.2.3).

[103] O'Malley, P. (2013) The politics of mass preventive justice, in Ashworth, A. et al. (eds.), *Prevention and the limits of the criminal law*, OUP, pp. 273-295

[104] See S. and Marper v. The United Kingdom, ECHR application no. 30562/04 and 30566/04, 4 December 2008, para. 122

[105] Richards, N.M. (2013) The dangers of surveillance, *Harvard Law Review*, vol. 126, pp. 1934-1965

[106] Working document 1, on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf, (last accessed 20.12.2013); Brown, I, Korff, D. (2009) Terrorism and the proportionality of internet surveillance, *European Journal of Criminology*, vol. 6, no. 2, pp. 119-134

[107] Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, (last accessed 1.11.2013)

2.3.2.1 Mass surveillance in the EU

This sub-section discusses mass surveillance programmes in the EU and their implications for the right to privacy of the individuals. There is evidence that mass surveillance programmes are used extensively in some Member States of the EU[108] and they enable intelligence services and law enforcement authorities to access, without an individual warrant, to a large volume of personal data.[109] The aim of this form of interference with the life of the individuals is to identify and avert serious dangers, such as an armed or terrorist attack that threaten the national security of a country as well as other criminal activities disturbing the public security.[110]

The difference between targeted surveillance and mass surveillance is that in one case, the interfering measure is directed towards an individual and related with a specific crime, while in the case of mass surveillance, the measure is more of a preventive nature and it is directed to an entire category of individuals. This makes mass surveillance programmes[111] more intrusive than targeted surveillance since they interfere largely with the life of innocent individuals, devoid of any suspicion, only on the basis of falling under a category, making use of certain ways of communication or of certain devices.[112] At European level, these surveillance measures find legitimization in the non-absolute nature of the protection regulated by article 8 ECHR,[113] allowing for interference with the private life of the individuals in a situation that is: "*in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*",[114] as well as articles 7 and 8 of the European Charter of Fundamental Rights.

Even if article 8 ECHR was originally intended to cover situations of targeted surveillance, the ECtHR extended its application and the test it has established on its basis for cases of individual surveillance to cases of mass surveillance. For the ECtHR there are no grounds to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual

[108] Ibidem; PACE Report on Mass surveillance (provisional version) from rapporteur P. Omtzigt, available online at: http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2 (last accessed 29.1.2015)

[109] Gamino Garzia, A. et al. (2014) Study on Mass Surveillance – Risks and opportunities raised by the current generation of network services and applications, presented at European Parliament Scientific Foresight (STOA) Unit, December 2014, available online at: http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Study%20Mass%20Surveillance%20Part%201.pdf (last accessed: 23.2.2015)

[110] Weber and Saravia v. Germany, ECHR application no 54934/00, 29 June 2006, para. 4

[111] Mass surveillance programmes are sometimes referred to also as "strategic monitoring"

[112] Drulakova, R. (2006) Post-democracy within the EU: Internal security vs. human rights – unavoidable conflict?, paper prepared for the CEEISA 4th convention, Tartu, 25-27 June 2006, available online at: http://www.ceeisaconf.ut.ee/orb.aw/class=file/action=preview/id=167766/Drulakova.doc, (last accessed 1.11.2013)

[113] Himma, K.E. (2007) Privacy vs. Security: Why privacy is not an absolute value or right, *San Diego Law Review*, vol. 45, p. 859; Kleining, J., Mameli, P., Miller, S., Salane, D., Schwartz, A. (2011) Security and Privacy: Global standards for ethical identity management in contemporary liberal democratic states, *ANU E Press*, p. 43

[114] See article 8(2) ECHR

communications or more general programmes of surveillance.[115] Since in most of the cases it is impossible for an individual to know or prove the fact that his private life has been interfered with mass surveillance measures, the ECtHR accepts complaints also from individuals that cannot prove to have been individually subject to such surveillance practices. In these cases, the individuals may challenge the national legislation which allows a system of mass surveillance.[116] Mass surveillance is considered as an interference with the right to privacy of the individuals protected by article 8(1) ECHR and the burden is on the State authorities to prove that their action is "in accordance to the law", it serves a "legitimate aim in a democratic society" and it is "necessary and proportionate" in respect to the legitimate aim.

At national level the legitimisation of such large-scale surveillance may differ from country to country. In some countries, it operates on the basis of orders, issued by special courts (as for example in Sweden). In other countries, it is legitimised on the basis of warrants issued by the government (the United Kingdom, the Netherlands), or by an authorisation of oversight bodies (Germany, France, the Netherlands).[117] According to a report of the European Parliament, mass surveillance programmes are promoting a mix of law enforcement and intelligence activities with unclear legal safeguards, which are not in line with democratic checks and balances and fundamental rights.[118]

Mass surveillance of citizens is not a new phenomenon. It is enough to recall the infamous secret services operating till not very long time ago in territories that are now part of the Member States of the Union as for example Stasi in the former Democratic Republic of Germany or UDBA in former Yugoslavia. The new technology independent of being built or not for the purpose of surveillance facilitates the latter. What should distinguish the new forms of mass surveillance existing today from the former ones as well as democratic regimes from police states, are the purpose and the scale of surveillance. However, at the moment there is a lack of knowledge about these issues in the existing mass surveillance programmes.

[115] Liberty and Others v. The United Kingdom, ECHR application no 58243/00, 1 July 2008, para. 63

[116] Weber and Saravia v. Germany App no 54934/00 (ECHR 29 June 2006), para. 78; Zakharov v. Russia, ECHR application no. 47143/06, 4 December 2015, para. 179; just complaining of potential surveillance in the absence of legal rules that introduce it is however not enough, see Esbester v. the United Kingdom, ECHR application no. 18601/91, Commission decision of 2 April 1993

[117] Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, (last accessed 1.11.2013)

[118] European Parliament A7-0139/2014, Report on the US NSA surveillance programmes, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Homme Affairs (2013/2188(INI)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, no 139 of 21.02.2014, para. 10

An analysis of mass surveillance programmes in five EU Member States[119] has shown that there is little transparency as well as information on the purpose limitation and scale of mass surveillance programmes. This lack of transparency, combined with the large scale of use, and the intensity of intrusion of these forms of surveillance with the private life of the individuals, questions their compatibility with the basic principles of a democratic society.[120] In this line of reasoning, Bigo, Carrera et al. (2013) also state that the analysis of mass surveillance in the EU cannot be reduced to a question of striking a balance between the protection of different interests, but has to be framed in terms of collective freedoms and the nature of the democratic regime.[121]

The passive subjects of surveillance covered by these programmes are broad (e.g. the UK´s GCHQ[122] identify as targets: diplomatic, military, commercial targets, terrorists, organised criminals, e-crime, cyber actors).[123] This makes mass surveillance measures to appear similar to "fishing expeditions": very broad enquires carried out in the hope that they will turn up some evidence of a planned crime where no such evidence exists in advance. As an untargeted investigation mass surveillance programmes are likely to be ineffective and are highly objectionable since they expose much of a population to surveillance. There is normally no reason to think that most of a population is contemplating criminal activity.[124] The large scale of surveillance is actually the reason why "fishing expeditions" have been ruled out by the Council of Europe legislative framework[125] for special investigation techniques.[126] In this light, the legitimisation of mass surveillance programmes in the EU would qualify as a paradox. This routine surveillance of citizens is evaluated not only as unnecessary because it does not reduce crime, but also as counterproductive because it makes it more difficult to

[119] Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, (last accessed 1.11.2013)

[120] Korff, D. (2013) Note on European and International law on trans-national surveillance prepared for the Civil Liberties Committee of the European Parliament to assist the Committee in its enquires into USA and European States' surveillance, available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf (last accessed: 1.11.2013)

[121] Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, (last accessed: 1.11.2013)

[122] GHCQ stands for the UK intelligence agency Government Communications Headquarters

[123] MacAskill, E., Borger, J., Hopkins, N., Davies, N., Ball, J. (2013) Mastering the internet: how GCHQ set out to spy on the world wide web, *The Guardian* (21 June 2013), available online at: http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet (last accessed: 2.11.2013)

[124] Sorell, T. (2011) Preventive policing, surveillance, and European counter-terrorism, *Criminal Justice Ethics*, vol. 30, no. 1, pp. 1-22

[125] Recommendation Rec(2005)10 of the Committee of Ministers to Member States on 'special investigation techniques' in relation to serious crimes including acts of terrorism, para. b(4)

[126] De Koster, P. (2005) Terrorism: special investigation techniques, CoE Publishing, p. 21

search for the "needle in the haystack" of untargeted data and at the same time it limits the freedoms of the citizens.[127]

In practice, the information collected via mass surveillance has been often used for connecting the dots, or bringing together, for example, information related with certain e-mail or IP addresses. [128] This use of the collected information from individuals that are easily identified blurs the distinction between mass surveillance and warrantless targeted surveillance. Stated differently, mass surveillance might go as far as to operate *de facto* as a legitimization of warrantless surveillance of targeted individuals.

The intelligence[129] gathered via mass surveillance programmes at a pre-trial phase (both metadata and content),[130] can be used as evidence during a trial phases if it fulfils the fair trial requirements of Article 6 ECHR.[131] Furthermore, the 2013 report finds that intelligence collected by mass surveillance programmes, in France and Sweden for example, is shared between national law enforcement and security bodies.[132] As a result, the data is being used in a wide range of security purposes and not only for the narrow focus of counter-terrorism and defence. In this way, bits and pieces of the private life of an individual, collected in the absence of an individual warrant and clear legal safeguards, might be retrieved and used retroactively during the various stages of a criminal process.

[127] Friedewald, M. (2010) Sorting out smart surveillance, in *Computer Law and Security Review,* vol. 26, pp. 343-354

[128] Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, (last accessed: 1.11.2013)

[129] Eijkman, Q., Van Ginkel, B. (2011) Compatible or incompatible? Intelligence and human rights in terrorist trials, *Amsterdam Law Forum*, vol. 3, no. 4, pp. 1-16

[130] For the UK and Sweden see National programmes for mass surveillance in Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, (last accessed: 1.11.2013)

[131] Coster van Voorhout, J.E.B. (2006) Intelligence as legal evidence – Comparative criminal research into the viability of the proposed Dutch scheme of shielded intelligence witnesses in England and Wales, and legislative compliance with Article 6(3)(d) ECHR, *Utrecht Law Review*, vol. 2, no. 2, pp. 119 – 144. For the Netherlands the Supreme Court has decided that intelligence may serve as evidence provided that there is no rule prohibiting such use of intelligence, PHR 5 September 2006 ECLI:NL:PHR:2006:AV4122, PHR 5 September 2006 ECLI:NL:PHR:2006:AV4144 and HR 5 September 2006 ECLI:NL:HR:2006:AV4149 – see footnote 68 in Coster van Voorhout

[132] See Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, (last accessed 1.11.2013), p. 24 and Annex 1 (Sections 3 and 4).

There is at the moment little transparency on the way mass surveillance programmes operate and their efficiency in the fight against terrorism and other crimes. We are also all unaware on the information that is known about us, if not actively, passively from the surveillance systems and devices. In a working document of the European Parliament, rapporteur Morales says about this that: "*By being able to collect data regarding the content of communications, as well as metadata, and by citizens' electronic activities, in particular their use of smart phones and tablet computers, intelligence services are de facto able to know almost everything about a person. They can know where people are with advanced location programmes, with whom they speak and for how long, what they do, what they buy, what they read and even what they think*."[133]

It is submitted that most of the time, mass surveillance programmes are automated and classify communications on the basis of the use of certain key words or of contacting a certain phone number, without the overview of the context in which a communication was done. In this way, more and more information is stored and recorded in the system and possibilities for false positives are present. Even if some information is prohibited from being used as evidence in a trial since it cannot meet the fair trial requirements, it will still be capable of influencing the approach of the law enforcement authorities and[134] the way the individual will be treated. It will certainly facilitate a channel by which the law enforcement authorities might discover other information,[135] or create parallel constructions of the facts.[136] No proper protection of citizens' right to privacy exists so far in the EU in the presence of mass surveillance programmes. The only possibility that the citizens have is to challenge their validity, but the European Court of Human Rights has taken a less active approach in such cases due to the margin of appreciation that is left to the Member States.[137]

[133] Working document 1, on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf (last accessed: 20.12.2013)

[134] Roach, K. (2010) The eroding distinction between intelligence and evidence in terrorism investigations, in McGarrity, N., Lynch, A., Williams, G. (eds.), *Counter-terrorism and beyond*, Routledge, pp. 48-68

[135] See Naughton, M. (2011) How the presumption of innocence renders the innocent vulnerable to wrongful convictions, *Irish Journal of Legal Studies*, vol. 2, no. 1, pp. 40-54, this author states that: "[…] *investigations often work from an approach* […] *termed "hypothesis in", i.e. finding evidence to support a predetermined hypothesis of guilt, rather than from the "facts out", i.e. neutrally assessing the evidence to ascertain what might have occurred*."

[136] In an article of Reuters in August 2013 it has been discovered a method used by the anti-drugs police in the USA to hide information they receive illegally from NSA and other intelligence units. This method is called "parallel constructions" and on the basis of it trained agents reconstruct the investigative trail to cover up where the information originated from. There is no evidence of the use of this method in the EU, but the information received illegally from mass surveillance programs can very well make it possible. See Shiffman, J., Cooke, K. (2013) US directs agents to cover up programme used to investigate Americans, *Reuters* (5 August 2013), available online at: http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 (last accessed: 10.2.2014)

[137] Liberty and Others v. The United Kingdom, ECHR application no. 58243/00, 1 July 2008, para. 68

2.3.2.2 Mass surveillance and data retention

After discussing mass surveillance in general, this sub-section focuses on the case of data retention in the EU. The Data Retention Directive[138] has a special role for the analyses since the interference with the life of the individuals it introduced is a form of mass surveillance from the State with the help of technology not built for the purpose of surveillance.[139] At the same time it represents also one of the many cases of surveillance with non-purpose collected data - data collected and retained for a certain purpose have subsequently changed the purpose of collection and are used for law enforcement purposes. The analyses of the Directive and the reasons for its invalidation will thus help to clarify the legal requirements for this form of interference with the life of the individuals in respect to the fundamental rights to privacy and data protection. That are the reasons this sub-section is dedicated to the adoption and invalidation of the Data Retention Directive.

2.3.2.2.1 Background information

The aim of the Data Retention Directive was to allow the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks for possible use by law enforcement authorities.[140] Essentially, providers of fixed and mobile telephony services and internet service providers were expected to retain records of service users to trace and identify the source, destination, date, time and duration of a communication together with information necessary to identify the type of communication, the equipment used and the geographical location of the user.[141] All this metadata was to be kept according to the time limit set by national law but for no less than six months and no more than two years.[142] The aim of the Directive was to ensure that the data retained by the service providers were available for the purpose of investigation, detection and prosecution of serious crime[143] – the latter as defined by each Member State in its national law.[144] The data retention was not done for a

[138] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[139] Maras, M.-H. (2009) From targeted to mass surveillance: Is the EU data retention directive a necessary measure or an unjustified threat to privacy, in Goold, B.J., Neyland, D. (eds.), *New directions in surveillance and privacy*, pp. 74-105

[140] For a detailed presentation of the reasons for the introduction of the Data Retention Directive please see: Mifsud Bonnici, J.P. (2007) Recent European Union developments on data protection … in the name of Islam or 'Combating terrorism', *Information & Communications Technology Law*, vol. 16, no. 2, pp. 161-175; Munir, A.B., Yasin, S.H.M. (2004) Retention of communications data: a bumpy road ahead, *Journal of Computer & Information Law*, vol. 22, pp. 731-758; Maras, M.H. (2011) While the European Union was sleeping, the data retention directive was passed: The political consequences of mandatory data retention, *Hamburg Review of Social Sciences*, vol. 6, no. 2, pp. 1-30; Kosta, E. (2013) The way to Luxemburg: National Court decisions on the compatibility of the data retention directive with the rights to privacy and data protection, *SCRIPTed*, vol. 10, no. 3, pp. 339-363

[141] Art. 5 Data Retention Directive

[142] Art. 6 Data Retention Directive

[143] Reidenberg, J.R. (2014) The data surveillance state in the United States and Europe, *Wake Forest Law Review*, vol. 49, pp. 583-608

[144] Rec. 21 Data Retention Directive. See also COM(2011) 255 final, Brussels, 18.4.2011, Evaluation Report on the Data Retention Directive; The Dutch law implementing the Data Retention Directive, was, for example

specific, limited purpose but it was general and continuous. As a result, the purpose-limitation principle that is central to data protection legislation was undermined.[145]

The Directive essentially introduced a form of mass surveillance (dataveillance)[146] of citizens at EU level.[147] This was based on the ability of service providers to collect and retain a number of personal data for different purposes (as for example billing details) and then use these data for other purposes, in the specific case, for mass surveillance of the users of electronic communications. There is an essential difference between the way the retention of data was done on the basis the Directive and other databases created at European level, as for example EURODAC, SIS II or VIS.[148] The scope of the Data Retention Directive was to benefit from the way of operation of electronic communications and it suggested to change the purpose of the data collected for service purposes and use them for law enforcement ones. Advancement in technology makes it easier in the future to use the same scheme as under the Data Retention Directive for the massive accessing of personal data collected for other purposes (as for e.g. in the case of smart meters).

Data collection and retention in this case was considered as one of the most privacy invasive instruments ever adopted by the EU.[149] It has an implication both for the right to privacy and the one to data protection.[150] To interfere with the right to privacy does not require necessarily that the information on the private lives concerned is sensitive but it is enough that the individual has been inconvenienced in a certain way.[151] This condition is fulfilled, according to the CJEU by the retention of the data as well as by the potential access by the national authorities. The processing of the personal data required by the Directive brings it automatically under the data protection regime since data processing is involved. The CJEU refers to personal data in relation to the protection of the right to privacy (as informational privacy) and considers that the protection of personal data is especially important for the right to respect for private life.[152] A lot of information can be discovered on the private life of an individual by processing personal data. In the case of the Data Retention Directive information can reveal the contacts of someone, how often he communicates with them, from whom someone seeks advise, how often, etc. The potential use of the data without informing

---

having a broad definition of serious crime including also bike theft. See para. 3.10 of the decision of the Court of the Hague RBDHA 11 March 2015 ECLI:NL:RBDHA:2015:2498

[145] Mifsud Bonnici, J.P. (2014) Redefining the relationship between security, data retention and human rights, in Holzhacker, R., Luif, P. (eds.), *Freedom, security and justice in the European Union*, Springer, pp. 49-74

[146] For an explanation of dataveillance see Clarke, R. (1997) Introduction to Dataveillance and Information Privacy, and Definitions of Terms, available online at: http://www.rogerclarke.com/DV/Intro.html (last accessed 22.5.2014)

[147] Roberts, H., Palfrey, J. (2010) The EU Data Retention Directive in an era of internet surveillance, in Deibert, R. et al. (eds.) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT, pp. 35 - 53

[148] The laws that introduce these databases are further discussed in chapter 3

[149] EDPS (2011) Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)

[150] UN OHCHR (2014) The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, para. 20

[151] Joint Cases C-465/00, C-138/01 and C-139/01 Rundfunk, para. 75

[152] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 53

the person concerned makes this interference particularly serious since "… *it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*".[153] This argumentation of the CJEU is related with the fact that this form of data retention turns surveillance for the individuals into a normal situation, a rule. In a time when new technologies have the potential to make collection and retention more easy to perform not just by systems designed for the purpose of surveillance, and the interference with the private life of the individuals becomes much more intrusive,[154] it is important to identify the reasons the European Court invalidated the Data Retention Directive and see if they can extend also to other surveillance with non-purpose built technology.

2.3.2.2.2 The invalidation of the Directive

The Court of Justice of the EU ended the long debate on the validity of the Directive and invalidated it finding that its interference with the articles 7 and 8 of the Charter was exceeding the limits imposed by the principle of proportionality.[155] The breach was considered by the CJEU so severe that, in difference from the opinion of the Advocate General,[156] the CJEU did not provide for a suspension of the effects of its judgment till the Member States would adopt the necessary legal acts required after its invalidation. The effects of the invalidation of the Directive for the EU were immediate and *ab intitio*.[157] As a result, the Directive is to be considered today as if it had never existed.

In its elaboration, the CJEU first identified the existence of the interference with the protected rights and then examined the possible justifications. It has to be noted, however, that despite finding an interference both with the right to privacy and the one to data protection, for the CJEU the essence of both rights is not considered as adversely affected and the Directive is considered to genuinely satisfy an objective of general interest. In this way, the CJEU left open the possibility for other legislation on data retention in the EU, provided that it would comply with the proportionality principle.

After establishing the interference with both fundamental rights, the CJEU continued by assessing the proportionality of the interference. The CJEU applied the proportionality test as established in its

[153] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238 , para. 37
[154] Marx, G. (2002), What is new about "New surveillance"? Classifying for change and continuity, *Surveillance and Society*, vol. 1, no. 1, pp. 9-29
[155] Article 52(1) of the Charter of Fundamental Rights of the EU
[156] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, Opinion of AG Cruz Villalon
[157] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238

earlier case law[158] composed of three steps: (i) appropriateness; (ii) necessity; and (iii) proportionality *stricto sensu*.[159]

In the first step the CJEU established if the measure is appropriate for attaining the set objectives.[160] The focus of the analyses is on the value that the retained data have for national authorities giving them additional opportunities to shed light on serious crime. Data retention methods are, therefore, evaluated as valuable for criminal investigation. What the CJEU is looking for at this stage is only that the retained data can have a value for law enforcement authorities. For the CJEU it is not relevant if these data are collected as a result of direct surveillance or are collected by devices and technology not built for surveillance purposes. As a result, a discussion on the means used for surveillance did not take place.

The CJEU discussed afterwards the second and the third step of the test (the necessity and the proportionality *stricto sensu* of the measure). In general, as it will be discussed more in detail in chapter 5 section 5.3.1.2, when analysing the proportionality of EU measures the CJEU looks at their "manifest disproportionality" while for national measures the test is stricter and focuses on the "less restrictive alternative". This biased approach might be justified with the fact that often national measures might be directed to individual cases and this facilitates a proportionality assessment while for EU legislation the separation of powers gives the CJEU a less prominent role.[161] This biased approach might also stand in the area of market integration[162] but does not have a reason to stand when analysing the infringement of fundamental rights of the individuals for which a strict approach is needed.[163]

The CJEU appeared to be aware of this. If the CJEU would have been following its established line of reasoning when assessing the proportionality of EU rules, it would have been limiting its reasoning to the "manifestly disproportionate" test. However, this was not the case for the Data Retention Directive. The CJEU referred to the case C-473/12 *IPI*[164] and used the formula stating that "…*derogations and limitations in relation to the protection of personal data must apply only in so far*

[158] Case 11/70 Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide [1970] ECR1125
[159] The proportionality test as applied by the CJEU is presented in detail in chapter 5 section 5.3.1.2. See also Troncoso Reigada, A. (2012), The principle of proportionality and the fundamental right to personal data protection: The biometric data processing, *Lex Electronica*, vol. 17.2, pp. 1-44
[160] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 49
[161] However, in a number of occasions the Court has been going beyond the wording of a provision, changing its meaning for extending the scope of application of EU law. See for example case C-617/10 Aklagaren v. Hans Akerberg Fransson EU:C:2013:280, were the CJEU gave an extended interpretation of the wording "implementation of EU law" against its own meaning
[162] Harbo, T.-I. (2010) The function of the proportionality principle in EU law, in European Law Journal, vol. 16, no. 2, pp. 158-185
[163] Case C-112/00 Eugene Schmidberger, Internationale Transporte und Planzuge v. Austria [2003] ECR I-5659, para. 74; Case C-73/07 Satakunnan Markkinapörssi and Satamedia [2008] ECR I-9831, paragraph 56, and Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, paragraphs 77 and 86
[164] Case C-473/12 Institut professionnel des agents immobiliers (IPI) v. Geoffrey Engelbert, Immo 9 SPRL, Gregory Francotte EU:C:2013:715

as is strictly necessary". The test used by the CJEU has an *ex post* approach focusing on the existence of clear and precise rules to govern the scope and application of the measure and the existing minimum safeguards introduced against the risk of unlawful access and use of personal data. The test does not suggest to the CJEU to discuss the nature of the technology used for surveillance.

The detailed reasons for which the CJEU decided the invalidation of the Directive are discussed below. The CJEU looks first at the scale of the interference, then at substantive concerns for the access to the data from national authorities and finally at technical concerns, on the requirements for the service providers. Each reason is discussed in turn:

Scale of surveillance[165]

The Directive covers all persons, all means of electronic communication, and all data. It interferes therefore with the fundamental rights of the entire European population. The Directive has the form of mass surveillance, where no exceptions are provided for persons for whom there is no evidence of suggesting that their conduct might have a link with a serious crime, or persons whose communications are subject to professional secrecy.

In addition, the provisions of the Directive have failed to establish any relationship between the retained data and threat to public security and no restriction was provided with regards to a time period, geographical zone or group of people. There was no limitation to persons who could contribute to the prevention, detection or prosecution of serious offences.

The scale of surveillance is so disproportionate that it would have sufficed for the CJEU to invalidate the Directive for infringing the right to privacy. The CJEU however goes further in its elaboration by assessing the data access from national authorities as well as the requirements for the service providers. This gives the impression that the scale of surveillance (mass surveillance in this case) in itself does not suffice for establishing the invalidity of a surveillance measure.[166]

[165] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, paras. 56-57

[166] Legal analyses from the Danish Ministry of Justice concluding that the Danish retention law is not affected by the CJEU ruling on the DRD, available (in Danish) on line at: http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf; see also the Dutch government reaction on national data retention laws after the CJEU ruling on the Data Retention Directive, available online at: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/11/19/tk-reactie-van-het-kabinet-naar-aanleiding-van-de-ongeldigverklaring-van-de-richtlijn-dataretentie.html

Substantive concerns for the access to the data from national authorities[167]

The Directive failed to lay down any objective criteria that could serve to determine the limits of the access of the competent national authorities to the retained data and their subsequent use. The Directive did not contain any substantive and procedural conditions to the access and subsequent use of the data nor did it provide that these procedures were to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto. The data retention period was not established on the basis of objective criteria for categories of data and it was not ensuring its limitation to what is strictly necessary.[168] In addition, the Directive did not provide for judicial or independent administrative body review whose decision would seek to limit access to the data to what is strictly necessary. No objective criteria were designed for establishing the period of retention of the data and no distinction was made on the nature of the data.

Technical concerns on the requirements for service providers[169]

Another reason for establishing the disproportionality of the Directive was that it did not introduce any particular level of security for the service providers. Furthermore, it gave them the possibility to have regard to economic considerations when determining the level of security to which they apply. In addition, there were no special requirements for the service providers to retain the data within the territory of the European Union. This can be especially problematic when the cloud service provider operates outside the jurisdiction of the EU and it is difficult to maintain the same level of safeguards as within the Union.

For these reasons, the Directive was declared as not being in conformity with the proportionality principle (Art. 52 of the Charter) and infringing, therefore, both the right to privacy and the one to data protection. The fact that the means of electronic communication are all not built for surveillance and that these devices are freely in the hands of the European citizens was neither questioned, nor discussed. This was the result of the CJEU discussing the necessity step of the proportionality test only within the reduced scope of the "*limited to what is strictly necessary*" analyses. This aims to ensure safeguards for limiting the effects of surveillance for the citizens and not to find if the concrete surveillance was necessary.

2.3.2.2.3 A reflection upon the CJEU decision in light of the technology used for surveillance

This sub-section will reflect on why the decision of the CJEU did not include in its decision a discussion of the technology used for data retention and on how to extend the proportionality test

[167] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, paras. 58-65
[168] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 64
[169] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, paras. 67-69

for including such a discussion. It is important to note at this point that the need for a discussion on the means of surveillance in the Data Retention Directive is not just introduced artificially for the scope of this research. The CJEU by itself in discussing the proportionality of the Directive (para. 57) declares that its provisions are referring in a generalized manner to "all persons", "*all means (of surveillance)"* and "all data". In continuing the discussion however, the CJEU elaborates on "all persons" (para. 58) and "all data" (para. 59) without referring anymore to "all means". This is first of all related with the CJEU limiting its attention to "what" is being surveilled – all electronic communications – without paying attention to the devices used for surveillance. Secondly this is related also with the CJEU making use of the "limited to what is strictly necessary" test. This test is used rarely[170] since when EU law is contrasted to individual rights the CJEU is normally focussing its attention on the "manifestly disproportionate" nature of the measure.[171] In the concrete case, the CJEU found the measure to be appropriate for reaching its aims, but since fundamental rights of the individuals were concerned and their limitation has to be interpreted in a strict way the CJEU reasons that the interference with the rights introduced by the EU legislator must apply "*only in so far as strictly necessary*".[172]

This reasoning from the CJEU is plausible. It is to be kept in mind that mass data retention affects primarily individuals that do not have any past, present or even future relation to a criminal activity. As a result, high safeguards as well as a strict proportionality test have to take place for non-compromising their fundamental rights. When defending mass surveillance of citizens, it is normally said that if one has nothing to hide than he has nothing to fear.[173] But in situations of untargeted surveillance a reasonable question would be: "If one has nothing to hide than why does the State look into one's private life?". Presently, it is continuous surveillance that one is experiencing and rightfully fearing.

Coming back to the discussion of the technology used for surveillance, the level of intrusion and awareness is different when using means that have been designed for the purpose of surveillance and when using non-purpose built technology. It has to be kept in mind as well that for devices built for the purpose of surveillance there are legal safeguards and awareness of the general public about their existence in those cases in which they are used in a not targeted way (for example there are signs indicating that an individual is entering a CCTV surveyed area of the city). As a result, an

[170] C-473/12 Institut professionnel des agents immobiliers (IPI) v. Geoffrey Engelbert, Immo 9 SPRL, Gregory Francotte EU:C:2013:715

[171] Tridimas, T. (1999), Proportionality in European Community law: Searching for the appropriate standard of scrutiny, in Ellis, E. eds., *The principle of proportionality in the laws of Europe*, pp. 65-84; C-84/94 United Kingdom v. Council [1996] ECR I-5755, para. 57; C-265/87 Schraeder HS Kraftfutter GmbH & Co KG v. Hauptzollamt Gronau [1989] ECR 2237, para. 21-24; Case C-331/88 The Queen v. Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa et al. [1990] ECR I-4023, para. 8; C-491/01 The Queen v. Secretary of State for Health, ex parte British American Tobacco (Investments) Ltd and Imperial Tobacco Ltd [2002] ECR I-11453, para. 123; Joined cases C-453/03, C-11/04, C-12/04 and C-194/04 ABNA Ltd et al. v. Secretary of Health et al. ECR I-10423, paras. 80-84

[172] Ovey, C., White, R. (2002) European Convention on Human Rights, OUP 3rd ed., p. 257

[173] Solove, D. (2011) Nothing to Hide: The False Tradeoff Between Privacy and Security, Yale University Press, p. 1

individual may regulate his behaviour accordingly. But the same does not happen with devices that we use daily for other purposes and that are slowly becoming existential parts of our lives (e.g. smart phones). Individuals are not informed on the surveillance capabilities of the devices they voluntarily acquire and that have the possibility to continuously and automatically collect personal data without the need of any warrant or warning. The knowledge and processing of the data collected can reach a high level of intrusion into the private life of the individual and presents a clear risk for the violation of his fundamental rights.[174] There is no other possibility for the individuals to adjust their behaviour apart deciding not to make use of devices and programmes and therefore deprive themselves from the technological advances, limit their freedoms, as for example the freedom of expression, and even undermine their social relations and the right to privacy itself.

In the Data Retention Directive case the CJEU is limiting the necessity step of the proportionality test to the "limited to what it is strictly necessary" analyses. The CJEU has however failed so far to clearly determine what is covered under the definition of necessity in a democratic society. Since in the case of the data retention the CJEU is assessing fundamental rights against EU public interests and the rights of millions of innocent people are interfered with, less restrictive alternatives should have been taken into account.[175] The proportionality test used by the CJEU, even if plausible, should have been going further, as to include the "less restrictive alternative" analyses.[176] This would have given to the CJEU the possibility to assess the technologies used for data retention. Even if the Charter of Fundamental Rights of the EU is hierarchically on the same level as the EU Treaties,[177] it is not disputable that fundamental rights of EU citizens would rank higher that market integration instruments.[178] The use of the "less restrictive alternative" criteria would have given the CJEU the possibility to properly use the proportionality principle for the protection of the fundamental rights of the individuals.

The "limited to what is strictly necessary" test does not open the doors for an assessment of the means used for surveillance since its aim is different. In the way this test has been used so far by the CJEU,[179] it does not assess the form of surveillance and the way it is done but its aim is to limit the impact of the interference with the life of the individual by evaluating the existing safeguarding measures. On the other side, the "less restrictive alternative" criteria, as the name suggests, aims to

[174] Cohen, N. (2011) It's tracking your every move and you may not even know, in The New York Times, 26 March 2011, available online at: http://www.nytimes.com/2011/03/26/business/media/26privacy.html?_r=0 (last accessed 22.5.2014)
[175] Feiler, L. (2010) The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection, European Journal of Law and Technology, vol. 1, no. 3, pp. 1-34; Docksey Ch. (2014) The European Court of Justice and the decade of surveillance, in Hijmans, H., Kranenborg, H. (eds.) Data protection anno 2014: How to restore trust?, pp. 97 - 111
[176] The "less intrusive alternative" is proposed also in UN General Assembly Report of the Special Rapporteur Ben Emmerson on the Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, 23 September 2014, paras. 51-52
[177] Article 6 TEU
[178] See Case C-301/06 Ireland v. Parliament and Council [2009] ECR I-00593 and Art. 6 TEU
[179] Case C-473/12 Institut professionnel des agents immobiliers (IPI) v. Geoffrey Engelbert, Immo 9 SPRL, Gregory Francotte EU:C:2013:715

show that the desired result cannot be achieved with other means that would interfere less with the rights of the individual. The application of this test might have as a result the limitation in the use for surveillance of non-purpose built technology that collects data. Since surveillance is related with a limitation of fundamental rights of the citizens, this study suggests that the CJEU uses the "less restrictive alternative" test when assessing the proportionality of European measures in this regard. The need for identifying the less intrusive alternative means is suggested also by the Court of Human Rights in the *Uzun* case were the use of a GPS device for controlling the car movements of the claimant was considered as proportionate given that the less restrictive alternatives were provided not to be successful.[180] One has to keep in mind that *Uzun* faced targeted surveillance and the less restrictive alternative is even more important when interfering with the rights of innocent citizens as in the case of data retention. The use of this criterion as part of the proportionality test will also give the possibility to assess the use of non-purpose built devices for surveillance and better safeguard the rights of the citizens.

The experience of the Data Retention Directive teaches a number of lessons with regards to surveillance of citizens with non-purpose built technology. Firstly, data retention does not fall only under data protection but also under privacy rules.[181] As a result, the introduction of rules that change the purpose of the data collected must be assessed also on the basis of the privacy test. Secondly, data retention creates the possibility to surveil citizens via dataveillance. Because of the reason that the collection of data from technology we use daily is continuous, such surveillance could qualify as ubiquitous. Thirdly, because of the principle of availability, retained data used for law enforcement purposes is seen as an appropriate measure independent of the fact that the data are originally collected for a different purpose. This might have implications for all the technology we use. Fourthly, the scale of interference with the life of the individuals is not in itself a sufficient ground for invalidation of interfering measures. Similar with the decisions from the Court of Human Rights,[182] attention is paid also to the existing safeguards for accessing the data and for the way the data are saved by service providers which might rectify the scale of surveillance. Fifthly, for the proportionality test to work properly, attention must be paid to the technology used for interfering with the life of the individuals. Sixthly, the requirement of a high level of protection applies with particular strength in cases where EU legislation foresees mass data collection, storage of the data of a very large number of unsuspected persons and access to and use of such data by law enforcement authorities.[183]

[180] Uzun v. Germany, ECHR application 35623/05, 2 September 2010, para. 78

[181] The differences and similarities between the rights to privacy and data protection are discussed in chapter 3.4.1

[182] Arai-Takahashi, Y. (2002), The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR, Intersentia, p. 14; Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 29

[183] Council of the European Union 9009/14 LIMITE, Information note from the general Secretariat of the Council to the Permanent Representatives Committee/Council, Brussels, 5 May 2014, available online at: http://www.statewatch.org/news/2014/may/eu-council-note-data-retention-judgment-9009-14.pdf

The same reasoning that the CJEU used for invalidating the Data Retention Directive was later used in the *Tele2 Sverige* case for establishing the disproportionality of any national legislation which, for the purpose of fighting serious crime, provides for the general and indiscriminate retention of metadata of all users relating to all means of electronic communication.[184] For the CJEU: "…*while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight*...".[185] It has to be pointed out though that also in this case the CJEU used the "limited to what is strictly necessary" test[186] leaving undiscussed the use of the specific technology as the least intrusive measure for surveillance.

2.3.2.3 Concluding remarks

In this sub-section, it was seen that mass surveillance of European citizens for intelligence or law enforcement activities is a reality in the EU. The fact that in some Member States data collected for one activity can be used for the other makes it more difficult for the individuals to protect their rights. On the other side, the possibility to use for the scope of mass surveillance non-purpose built but surveillance-ready devices as well as non-purpose collected data increases and facilitates the possibilities for such a form of surveillance. The main safeguard that individuals in the EU presently have is to challenge the existence of mass surveillance programmes independent of being caught from one of them or not.

Mass surveillance conflicts with the right to privacy of individuals independent from the fact that the data collected are further used or not. The CJEU in the invalidation of the Data Retention Directive case stated that data retention, as a form of mass surveillance, is appropriate for the scope of prevention, detection and punishment of crime. It however conflicts with the rights to privacy and data protection of European citizens when disproportionate. For establishing the proportionality of such measures, it introduced a number of safeguards that are based on the scale of surveillance together with the access to the data and their storage by service providers. If these safeguards are not respected mass surveillance programmes are considered as infringing the articles 7, 8 and 52 of the Charter.

2.3.3 The time of surveillance and the principle of presumption of innocence

As already seen, surveillance with non-purpose built devices apart the possibility of direct surveillance has also the possibility, via dataveillance, to look into past activities of an individual, performed at a time one was not yet a suspect of crime, or even to predict future behaviour. Devices that are in our hands daily have the potential to collect data related to our activities. These data

[184] Joined cases C-203/15 and C-698/15 Tele2 Sverige EU:C:2016:970, para. 112
[185] Joined cases C-203/15 and C-698/15 Tele2 Sverige EU:C:2016:970, para. 103
[186] Joined cases C-203/15 and C-698/15 Tele2 Sverige EU:C:2016:970, para. 96

might then become important in a second moment, when the individual is suspected of having committed a crime. The aim of this sub-section is to assess the effects that surveillance into the private life of the individuals at a time in which they were not accused or suspected of having committed a crime has apart for their right to a protected private life, also for their right to presumption of innocence.

The development of technology has certainly changed our society. One may argue that currently there is a shift from a post-crime to a pre-crime society, based on risk assessment, suspicion and pre-emption.[187] In this pre-crime society suspicions are not based any longer on criminal behaviour but largely on marginal behaviour and life-styles.[188] As nicely put by Clarke (2015) the proponents of non-targeted surveillance apply "*the 'original sin' tenet (you're all guilty – we're just not sure what of yet)*".[189] While it is clear that retroactive surveillance interferes with the private sphere of the individuals at a time in which there was not a legitimate mandate for such an interference, in the following sub-sections are discussed in detail the effects that this privacy invasion creates to the right of presumption of innocence. First presumption of innocence and its time extension is discussed (sub-section 2.3.3.1), and then the focus shifts on the effects that surveillance with non-purpose built technology has on the principle (sub-section 2.3.3.2). It is concluded that surveillance with non-purpose built devices and non-purpose collected data in a period of time in which the individual was not yet a suspect of crime, undermine the application of the principle of presumption of innocence at the stages of a criminal process (sub-section 2.3.3.3).

2.3.3.1 Presumption of innocence[190]

The principle of presumption of innocence is one of the fundamental principles of a criminal law procedure. With its earlier examples in the code of Hammurabi (1772 BC), we find it included in all the most important international documents on human rights of our days, as for example: the Universal Declaration of Human Rights (article 11), the European Convention of Human Rights (article

[187] Morariu, M. (2009) How secure is to remain private? On the controversies of the European Data Retention directive, *Amsterdam Social Science*, vol. 1, no. 2, pp. 46-65; Fenwick, H., Phillipson, G. (2011) Covert derogations and judicial deference: Redefining liberty and due process rights in counterterrorism law and beyond, *McGill Law Journal*, vol. 56, no. 4, pp. 863-918

[188] Bowden, C. (2013) The US surveillance programmes and their impact on EU citizens' fundamental rights, *Briefing Note submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at:
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf (last accessed: 1.11.2013), the term "marginal behaviour" stands here for minimal or negligible behaviour as for example constructing the profile of an individual on the basis of the search terms he uses in a search engine

[189] Clarke, R. (2015) Data retention as mass surveillance: The need for an evaluative framework, in *International Data Privacy Law*, available online at:
http://idpl.oxfordjournals.org/content/early/2015/01/23/idpl.ipu036.full.pdf+html (last accessed: 11.1.2016)

[190] The challenges that surveillance with non-purpose built technology presents for the principle of presumption of innocence are presented in more detail in: Milaj, J., Mifsud Bonnici, J.P. (2014) Unwitting subjects of surveillance and the presumption of innocence, *Computer Law & Security Review*, vol. 30, no. 4, pp. 419-428

6(2)), the Charter of Fundamental Rights of the EU, (article 48), etc. The wording of the relevant provision in all these legal acts is very similar:

"*Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law*" (article 6(2) ECHR)

At the core of this principle is the procedural safeguard on the basis of which the accuser has the burden to proof the guilt of the accused, while the later does not have the burden to prove its innocence though certainly has all the rights to do so.[191] According to Ulväng (2013),[192] presumption of innocence concerns a number of meta-rules and it is used by the Courts as:

- a principle of objectivity (for judges and juries);[193]
- a right against self-incrimination (including the right to remain silent);[194]
- a burden of proof (on the accuser);[195]
- a high epistemic standard of proof (beyond any reasonable doubt);
- an obligation to acquit defendants if the standards are not met (*in dubio pro reo*);
- protection against courts´ rulings written in an insulting or chicane manner;[196]
- an obligation to treat defendants with respect.[197]

All these elements help to understand the central role that the principle has in a criminal process, for safeguarding the fairness of the latter.

Although the wording of the legal provisions refer to the use of the principle in the presence of a criminal charge (article 6.2 ECHR, article 48 CFREU), there is an ongoing debate within the doctrine as to the stages of the criminal process in which this principle operates or, said differently, whether it

[191] Trechsel, S. (2006) The right to be presumed innocent, in Trechsel, S., Summers, S. (eds.), *Human rights in criminal proceedings*, OUP, pp. 153-191
[192] Ulvang, M. (2013) Presumption of innocence versus a principle of fairness, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 205-224
[193] Barbera, Messegue and Jabardo v. Spain, ECHR application no. 100588/83, 10589/83 and 10590/83, 6 December 1988, para. 77
[194] Saunders v. UK, ECHR application no. 19187/91, 17 December 1996, para. 69; Heaney and McGuinness v. Ireland, ECHR application no. 34720/97, 21 December 2000, para. 40
[195] Barbera, Messegue and Jabardo v. Spain, ECHR application no. 100588/83, 10589/83 and 10590/83, 6 December 1988, para. 77
[196] Rushiti v. Austria, ECHR application no. 28389/95, 21 June 2000, para. 27; Sekanina v. Austria, ECHR appication no. 13126/87, 25 August 1993, para. 30
[197] Barbera, Messegue and Jabardo v. Spain, ECHR application no. 100588/83, 10589/83 and 10590/83, 6 December 1988, para. 77

may actually operate outside a criminal process.[198] This debate is relevant for us since in cases of surveillance with non-purpose built technology and especially in cases of dataveillance, the surveillance goes back in time into the life of the individual before any criminal process was initiated. The ECtHR rulings have contributed to the debate, since the Court has extended the application of the principle of presumption of innocence outside the strict frames of a legal process.[199]

For the ECtHR, the principle applies also at the pre-trial stage of a criminal procedure,[200] as soon as the individual is formally informed about the criminal charge.[201] A formal accusation is, however, not considered by the ECtHR as a pre-requisite, since a substantive rather than a formal conception of criminal charge is taken into account.[202] The application of the principle has been extended by the ECtHR to apply also to witnesses whenever they are in reality suspected of having committed a crime, since the formal qualification of the individual is irrelevant.[203] In the same line, the ECtHR has considered presumption of innocence to be infringed not only by a judge or court, but also by other public authorities outside a court.[204]

The extensive interpretation given by the ECtHR is reflected in the new Directive adopted for harmonizing national laws with regards to the application of presumption of innocence principle.[205] This Directive was initiated in the context of the Stockholm Programme[206] with the aim to introduce common minimum standards on fair trial rights. The provisions of the Directive leave open the period of time in which presumption of innocence commences to operate. According to article 2 of the Directive, the application of the principle is extended also to suspects, so also in a pre-trial phase. The application is however linked with a specific criminal proceeding. Thus, the protection of the law does not apply to individuals that face interference with their private life outside a criminal proceeding or on the basis of mass surveillance programmes.

---

[198] Duff, A. (2013) Who must presume whom to be innocent of what?, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 170-192; Weigend, T. (2013) There is only one presumption of innocence, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 193-204; Knigge, G. (2013) On presuming innocence, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 225-238; Taipale, K.A. (2005) The trusted systems problem: Security envelopes, statistical threat analysis, and the presumption of innocence, *IEEE Intelligent Systems*, vol. 20, no. 5, pp. 80-82; Hirsch Ballin, M. (2008) An inside view of Dutch counterterrorism strategy: countering terrorism through criminal law and the presumption of innocence, *The Journal of the Institute of Justice and International studies*, vol. 8, pp. 139-151; see also Tadros, V. (2007) Rethinking the presumption of innocence, *Criminal Law and Philosophy*, vol. 1, pp. 193-213

[199] Salduz v. Turkey, ECHR application no. 36391/02, 27 November2008, para. 50-52

[200] Salduz v. Turkey, ECHR application no. 36391/02, 27 November2008, para. 50-52

[201] Deweer v. Belgium, ECHR application no. 6903/75, 27 February 1980, para. 44-46; Adolf v. Austria, ECHR application no. 8269/78, 26 March 1982, para. 30-31

[202] Foti and others v. Italy, ECHR application no. 7604/76, 10 December 1982, para. 52; Adolf v. Austria, ECHR application no. 8269/78, 26 March 1982, para. 30

[203] Brusco v. France, ECHR application no. 1466/07, 14 October 2010, para. 47

[204] Allenet de Ribemont App no 15175/89 (ECHR, 10 February 1995) para. 36

[205] Directive 2016/343 of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, pp. 1-11

[206] The Stockholm Programme — An open and secure Europe serving and protecting citizens, OJ C 115, 4.5.2010, 1-38

From the existing debate on the principle of presumption of innocence one can distinguish two main streams of thought. One of them is based on the letter of the law while the other one is detached from the statutory provisions. Despite the non-limitation of the application of presumption of innocence to the formal stages of a criminal process, individuals whose private lives are intruded, at a time in which they were not associated to a crime, cannot benefit from the procedural safeguards introduced by the principle if one considers its application linked with the existence of a specific criminal charge. This is the dominant point of view in the doctrine, and it is supported also by the case law of the European Court of Human Rights and the new Directive on presumption of innocence. However, individuals could benefit from the principle if the second line of reasoning is used and presumption of innocence is considered in a detached way, not bounded by statutory requirements.[207] In the rest of this sub-section the dominant interpretation of presumption of innocence is used since this conforms with ECtHR decisions and the new Directive. In other words, the principle is considered as linked with the existence of a specific criminal charge and therefore individuals that are outside such a framework - as for example in those situations in which surveillance is used for preventive purposes - do not benefit directly from it. It is claimed, however, that because of the possibility for retroactive surveillance that non-purpose built technology presents, the operation of the principle as a procedural safeguard through the stages of a criminal process is undermined.

With regards to mass surveillance programmes, the relationship between them and presumption of innocence was recently recognized in a report from the European Parliament.[208] This recognition from policy makers at EU level shows the different perception of the link between interference with the life of innocent citizens and the principle of presumption of innocence between the doctrine, the judiciary and the policy makers. In this case the policy maker's recognition of societal needs may very well anticipate later developments in the laws and the doctrine.

2.3.3.2 Presumption of innocence and surveillance

The principle of presumption of innocence, operating after a criminal charge was initiated, would give the individual the right to remain silent,[209] not to incriminate himself and leave to the accuser the burden to prove his guilt.[210] However, due to the possibility for retroactive surveillance which has increased with the use for surveillance of non-purpose built technology a lot of personal information

[207] Duff, A. (2013) Who must presume whom to be innocent of what?, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 170-192; Dijk, A., van (2013) Retributivist arguments against presuming innocence, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 249-267

[208] European Parliament A7-0139/2014, Report on the US NSA surveillance programmes, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Homme Affairs (2013/2188(INI)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, no 139 of 21.02.2014, para. 10 and 20

[209] Green Paper presented by the Commission, The presumption of innocence, COM(2006) 174 final, Brussels 26.4.2006

[210] Murray v. The United Kingdom, ECHR application no. 18731/91, 8 February 1996, para. 45

is in the hands of intelligence and law enforcement bodies and exchanged among them even before one is incriminated or suspected of having committed a crime.

The individual, on the other side, is unaware on the precise data and information that the accuser knows about his private life and actions. Furthermore, some of the evidence gathered with this form of surveillance at a time in which the individual was not a suspect, and therefore was not protected by the presumption of innocence principle, as for example voice or video recordings, are almost un-rebuttable. As a result, the usefulness of the protection that presumption of innocence offers in a criminal process is being questioned. Technology facilitates the existence of such evidence, independent from the individual will and such situations, according to the ECtHR do not qualify as infringements of the right that one has not to incriminate himself in a criminal trial.[211]

The possibility created for retroactive surveillance is *de facto* overturning the burden of proof during the stages of a criminal process from the accuser to the accused. Because of the lack of transparency and the information asymmetry between the accuser and the accused, presumption of innocence cannot serve anymore as a procedural safeguard for the individual in the era of surveillance with non-purpose built technology. For the reason that it is easy to retrieve information belonging to past activities, the accused needs to prove from the beginning of an investigation that he is not involved with a crime in order to have effective protection and perhaps avoid wrongful conviction.[212]

2.3.3.3 Concluding remarks

In this sub-section it was argued that surveillance with non-purpose built devices in a period of time in which the individual was not yet a suspect of crime, undermines the application of presumption of innocence in the stages of a criminal process. As a result, the principle presents itself in a diluted form that compromises the effectiveness of the legal process. Due to these forms of surveillance of individuals at a time in which they are devoid of any particular suspicion, once a criminal charge is made, the central role that presumption of innocence occupies for safeguarding the fairness of a criminal process, especially with regards to the right to remain silent and the burden of proof on the accuser, is compromised.

There are a number of elements that bring us to such a conclusion. They are related with the missing legal safeguards, the lack of transparency of the surveillance programmes, the exchange of information between intelligence and law enforcement bodies and especially, the information asymmetry between the accused and the accusers. The individual is not in control of his own data and is even unable to establish which information from his private life is known by the accusers. As a result, the individual cannot benefit *de facto* from some of the procedural guarantees that are at the

[211] Saunders v. The United Kingdom, ECHR application no. 19187/91, 17 December 1996, para. 69
[212] Naughton, M. (2011) How the presumption of innocence renders the innocent vulnerable to wrongful convictions, *Irish Journal of Legal Studies*, vol. 2, no. 1, pp. 40-54

heart of a fair process and presumption of innocence, as for example the right to remain silent. The burden of proof is also *de facto* shifted already in the very first stages of a criminal process, from the accuser to the accused. The lack of knowledge on the details of the information known on the individual private life should make him active from the first stages of a process to prove his innocence.

Regarding the possibility of presumption of innocence to offer protection to individuals in a situation in which they are not yet charged with a specific crime, but are still subjects of surveillance, there are a number of diverging opinions in the doctrine. The prevalent opinion, in line with the European Court of Human Rights rulings, is that presumption of innocence needs to be linked with a specific criminal charge, but can operate also outside a formal trial, as for example with regard to witnesses and individuals whose criminal charge, even if official, is not yet formalized. However, the recent recognition of the link between mass surveillance programmes and presumption of innocence in a report from the European Parliament,[213] anticipates new developments in the law and the doctrine in this regard.

In conclusion, it can be said that the classical understanding and safeguards of the principle of presumption of innocence as well as of the fair legal process in general are challenged in our society by retroactive surveillance which is facilitated by the use of non-purpose built technology. These forms of interference with the private life of the individuals do not only question the fundamentals of a democratic society, but also undermine the role of the principle of presumption of innocence at the stages of a criminal process, compromising the very effectiveness of the legal system.

2.4 Discussion and conclusion

This chapter identified the differences that surveillance with non-purpose built technology and traditional surveillance have in the form of legal challenges for the protection of the fundamental right to privacy of the individuals. Surveillance with non-purpose built technology is defined for this study as all State surveillance via technology and devices that have not been originally built for the purpose of surveillance. This surveillance can take the form of direct surveillance or dataveillance. Surveillance via data that have not been originally collected for the purpose of surveillance but used afterwards for this scope, as in the case of Data Retention Directive, is considered also as part of surveillance with non-purpose built technology.

Surveillance with non-purpose built technology differs from traditional surveillance in the way it interferes with the right to privacy of individuals. These differences consist in: (1) the active subject

[213] European Parliament A7-0139/2014, Report on the US NSA surveillance programmes, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Homme Affairs (2013/2188(INI)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, no 139 of 21.02.2014

of surveillance - changing the very understanding of surveillance from a vertical activity to one that is performed horizontally and, at times, even as self-surveillance; (2) the passive subject of surveillance - creating more possibilities for untargeted mass surveillance as well as for incidental surveillance; (3) the way surveillance is performed - increasing the role of dataveillance; (4) the aspects of the private life - increasing the level of their interference; and (5) the time of surveillance – making surveillance an activity that is not limited in observing the present but that can easily work retroactively for retrieving and analysing past activities of the individual, and even allowing for predictions of future behaviours. For these distinguished characteristics in the way it interferes with the private life of the individual surveillance with non-purpose built technology has to be considered as a specific form of surveillance. The distinction of the two categories of surveillance is reflected also in the challenges created for the protection of the right to privacy.

Surveillance in general endangers the right to a protected private life of citizens, but surveillance with non-purpose built technology has special implications with regards to an increase of cases of incidental surveillance, extended use of mass surveillance and the possibility for retroactive surveillance. Thus far there is not proper protection of the right to privacy of EU citizens when they find themselves in a situation of incidental surveillance. The case law from the European Court of Human Rights indicates that the citizens in these situations are even less protected than the ones that were the subject of targeted surveillance. The use of non-purpose built technology for surveillance must, therefore, keep in mind the effects this might have for the right to privacy of incidentally involved parties.

Mass surveillance is also to be seen as a threat to privacy since in these cases there is interference with the lives of millions of innocent citizens that do not have any past, present and even future connection with crime. Mass surveillance activities are currently covered by lack of information and under their umbrella are potentially covered also illegal surveillance actions of law enforcement. The invalidation of the Data Retention Directive by the Court of Justice of the EU considered mass data retention as being disproportionate and thus infringing the rights to privacy and data protection due to the scale of surveillance and not introducing certain safeguards on the access to the data as well as the way the data are stored by service providers. It is not clear however if the same reasoning would apply also for other general mass surveillance programmes.

The timeframe of surveillance, with the possibility to observe, thanks to the retained personal data, also a period of time in which the individual was not under suspicion, apart interfering with the right to privacy has an effect also for the principle of presumption of innocence and the fairness of the legal process. Due to the possibility of retroactive surveillance, not only the right to privacy but also the principle of presumption of innocence presents itself in a diluted form and cannot properly protect the rights of the individual in a criminal process.

In a discussion on the technology used for surveillance one has always to keep in mind that the protection of the right to privacy of the individuals in the EU is not an absolute one. It can be limited in the presence of need for protecting other values of a democratic society in the respect of the necessity and proportionality principles. Also the use of technology for surveillance must follow the same logic. The protection of the right to privacy of the individuals as a fundamental right requires however that the least interfering measure with their private sphere is used. Apart the written legal safeguards also the correct application of the proportionality principle must guide the choice of the surveillance measures in concrete cases. The role of the proportionality principle as a safeguard for the protection of the right to privacy of the citizens and for establishing the right balance between different rights is discussed further in chapter 5.

From this chapter it can be thus concluded that surveillance with non-purpose built technology is different from traditional surveillance and presents additional challenges to the protection of the right to privacy of the individuals. The ways these challenges are addressed thus far leave the right to privacy of the individuals unprotected. After this targeted analyses, the next chapter takes a holistic approach and identifies the European rules that are relevant for the protection of the right to privacy of European citizens and that apply in cases of surveillance. The reason for this analysis of the legal framework is to identify other provisions or principles that would aid the protection of the right to privacy of the individuals in situations of surveillance with non-purpose built technology.

Chapter 3 The European legal framework and the protection of the right to privacy of individuals for cases of surveillance with non-purpose built technology

3.1 Introduction

This chapter takes a holistic approach in identifying the legal framework applicable at European level for safeguarding the right to a protected private life of the individuals. This identification of legal provisions is, however, not done with the scope to simply catalogue the laws. The aim and the challenge of this chapter is to assess if the European legal framework that applies to traditional surveillance covers also the challenges that surveillance with non-purpose built technology creates. Particular attention is paid to the identified challenges of incidental surveillance, mass surveillance and retroactive surveillance. Since for reasons of flexibility, innovation, and harmonization, most of the legal rules are designed in a technology neutral fashion,[214] due attention is paid to the underlining principles that apply in the case of surveillance with technologies not built for the purpose of surveillance.

When talking about the legal framework applicable at European level, one might immediately think of the European Union Treaties, the Charter of Fundamental Rights of the EU that stands at the same hierarchical level with them,[215] the secondary legislation and the soft law. In this chapter, however, also a number of legal acts adopted at the Council of Europe level are discussed. The choice to include Council of Europe legal acts in a chapter about the European legal framework is supported by different reasons. Firstly, the right to a protected private life was first introduced in Europe via the European Convention of Human Rights.[216] As a result, a discussion of Council of Europe legal acts will help to historically understand the development of the right. Secondly, all Member States of the EU are also members of the Council of Europe and therefore they are bound by its provisions. EU citizens as well derive protection from Council of Europe legal acts.[217] Thirdly, the rights contained in the Convention are accepted in the EU as general principles of law that guide its operation and the adoption of legal rules. They represent the common legal tradition of the Member States.[218] Furthermore, in article 52(3) Charter of Fundamental Rights of the EU is stated that for rights which correspond to the rights of the Convention "*the meaning and scope of those rights shall be the same as those laid down in the Convention*". The interpretation of the Convention is therefore important

[214] It is sometimes argued, however, that pure technology neutral laws are just a myth since legislation is always adopted with some technology in mind. See: Birnhack, M. (2013) Reverse engineering informational privacy law, *Yale Journal of Law and Technology*, vol. 15, no. 1, pp. 24-91; Ohm, P. (2010), The Argument Against Technology-Neutral Surveillance Laws, *Texas Law Review*, vol. 88, pp. 1685-1713
[215] Article 6 TEU
[216] See article 8 ECHR
[217] For the complete list with the 47 Member States to the Council of Europe see: http://www.coe.int/en/web/portal/47-members-states
[218] Case 29/69 Stauder [1969] ECR 419

for interpreting the provisions of the EU Charter. Fourthly, EU legal acts often incorporate legal acts from the Council of Europe and refer to these acts for observance by the Member States.[219] The last but not the least reason for discussing Council of Europe acts together with EU ones is to understand the historical development of the right to data protection and its similarities and differences with the right to privacy.

At a first glance into the realm of EU secondary legislation, it is noticeable that most of the legislation initiated for the protection of the privacy of EU citizens in reality refers to data protection principles rather than to the right to privacy itself. One reason for this is of course the historical development of the right to data protection from the right to privacy and the fact that the two rights were officially separated only with the adoption of the Charter of Fundamental Rights[220] in 2000 and its having full legal effect after the entry into force of the Lisbon Treaty in 2009. Even if today it is generally accepted that the two rights are distinguished from each other,[221] it is still important to assess in how far the legislation on data protection does also protect the right to privacy of European citizens. The discussion on the distinction of the right to privacy from the one to data protection and the way this is reflected in the legal acts, case law and the doctrine will organically follow the assessment of the different legal instruments operating at EU level. It is to be kept in mind that these two rights are often overlapping with each other and that they are sometimes even used interchangeably.[222]

After this introduction, in section 3.2 the development of the right to privacy in the Council of Europe context is discussed. Article 8 ECHR will be interpreted and assessed with the help of the very rich body of judicial decisions from the ECtHR. In section 3.3, the secondary legal acts from the Council of Europe are discussed. The discussion of these acts will introduce the discussion on the distinction between the rights to privacy and data protection. In section 3.4, the distinction of the two rights in the European Charter of Fundamental rights will be complemented and discussed in light of the doctrinal debate and the decisions of the CJEU. The aim of this section is to establish the link between the two rights for the purpose of protecting the individuals' rights. The findings of this section will help in section 3.5 for discussing the primary and secondary legal acts at EU level. Attention in this latter section is paid not only to legal acts that have as purpose the protection of the rights of the individuals, but also to legal acts that introduce some sort of surveillance (dataveillance) of the individuals at EU level. In section 3.6 is discussed the new data protection reform packages and the implications that this has for surveillance with non-purpose built technology. A discussion of the legal framework and the conclusions are compiled in section 3.7. This section will attentively bring together the findings about the rules that apply to surveillance with non-purpose built technology in the EU and will assess its adequacy for safeguarding the rights of the individuals.

[219] See for example Council Decision 2005/876 on the exchange of information between the Member States from the criminal record, Art. 14; The Stockholm Programme – an open and secure Europe serving and protecting citizens 2010/c 115/01; COM(2010)609 final – Communication from the Commission to the EP, the Council, the ECOSOC and the CoR – A comprehensive approach on personal data protection in the European Union

[220] See articles 7 and 8 Charter of Fundamental Rights of the EU, OJ C 326, 26.10.2012, p. 391–407

[221] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007

[222] Klitou, D. (2014) Privacy Invading Technologies and Privacy by Design, Springer, p. 28

3.2 The right to a protected private life – the ECHR context

In Europe, the right to privacy was first included in the European Convention of Human Rights, article 8.[223] The wording of this provision, however, does not mention explicitly such a right, but four different, not mutually exclusive, areas of personal autonomy, namely: private life, family life, home and correspondence – that are considered as a projection of the right to privacy.[224] Despite the large number of decisions of the ECtHR based on this article, a conclusive definition of the right to privacy cannot be found even in the case law. This is however a clear choice of the ECtHR which has reiterated in a number of judgments that it is neither necessary, nor possible to give an exhaustive definition of what is understood with "private life".[225] "Private life" is considered to be a broad term whose content needs to be established on a case by case basis. To give just an example - also data collected in a public space and concerning exclusively professional or public activities of an individual are considered to fall within the private life sphere protected by article 8(1) ECHR in those cases in which the collection and storing of the data is done systematically.[226] The arbitrary State interferences with the private sphere of the individuals are limited for this study to those that qualify as surveillance activities.

The application and interpretation of the right to a protected private life from the ECtHR is relevant for the application of the right at EU level, since, as already stated, the meaning and the scope of EU fundamental rights included in the Charter is the same with the ones included in the European Convention of Fundamental Rights.[227] In its decisions the ECtHR clarifies that the right to private life cannot be limited to the protection of the "inner circle" in which an individual may live his own personal life as he chooses, but it is extended to the right to establish and develop relationships with other human beings, even in a public or professional context.[228] Interception of communications, for example, has been considered by the ECtHR to amount to an interference with the private life and the correspondence of the individuals.[229] Such interference, regardless to the aim to be achieved, is

[223] Article 8 ECHR *"Right to respect for private and family life"* reads:
"1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[224] In this research as well as in the EU legal framework, the terms "private life" and "privacy" are often used interchangeably. See the discussion of the terms in Gonzalez Fuster, G. (2014), The emergence of personal data protection as a fundamental right of the EU, Springer, p. 10

[225] Niemietz v. Germany, ECHR application no. 13710/88, 16 December 1992, para. 29; Peck v. The United Kingdom, ECHR application no. 44647/98, 28 January 2003, para. 57; Pretty v. The United Kingdom, ECHR application no. 2346/02, 29 April 2002, para. 61

[226] Shimovolos v. Russia, ECHR application 30194/09, 28 November 2011, para. 64

[227] See Article 52(3) Charter of fundamental Rights of the EU

[228] Niemietz v. Germany, ECHR application no. 13710/88, 16 December 1992, para. 29; P.G. & J.H. v. The United Kingdom, ECHR application no. 44787/98, 25 September 2001, para. 26; Halford v. The United Kingdom, ECHR application no. 20605/92, 25 June 1997, para. 44; White, R.C.A., Ovey, C. (2010), The European Convention on Human Rights, Oxford University Press, fifth edition, p.359

[229] Klass v. Germany, ECHR application no. 5029/71, 6 September 1978, para. 41; Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 77

not allowed unless it is done in accordance with the law, pursues one or more of the legitimate aims referred to in paragraph 2 of article 8 ECHR, and is necessary in a democratic society.[230]

Article 8 ECHR is framed in a technology neutral fashion. Such a choice gives the possibility to the law, via the means of interpretation, to cover new situations that were not yet envisaged at the time the provision was drafted. This is especially important in those areas that have a direct link with the continuous development of technology and this makes it difficult for the legal provisions to keep up to speed with the new developments.[231] As such, also surveillance with non-purpose built technology is covered by the protection of Article 8 ECHR.

Although the Convention is not specifically mentioning types of surveillance systems, the ECtHR's case law has dealt with different situations and applied article 8 ECHR in a myriad of cases. Examples include telephone conversations,[232] telephone metering,[233] voice recording,[234] e-mails,[235] etc.[236] The way the ECtHR has adapted to new situations and brought them into the realm of application of article 8 ECHR shows the dynamic character of the Strasbourg case law and underlines its determination to interpret the Convention as a "living instrument" able to deal with new situations.[237] The broad interpretation of the article gives the possibility to protect the private sphere of individuals from arbitrary interferences of the State independent from the technology used.

The obligation from the State not to interfere arbitrarily with the right of the individuals is a vertical one. This should not be understood, however, only as a negative obligation. In *von Hannover*[238] the ECtHR declared that the State has also positive obligations inherent in an effective respect for private or family life.[239] These obligations may include the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves, i.e. in a

[230] Huvig v. France, ECHR application no. 11105/84, 24 April 1990, para. 25
[231] Brakel, R., van, De Hert, P. (2011) Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Cahiers Politiestudies*, vol. 3, no. 20, pp. 163-192
[232] Klass v. Germany, ECHR application no. 5029/71, 6 September 1978
[233] Malone v. The United Kingdom, ECHR application no. 8691/79, 2 August 1984
[234] P.G. & J.H. v. The United Kingdom, ECHR application no. 44787/98, 25 September 2001
[235] Copland v. The United Kingdom, ECHR application no. 62617/00, 3 April 2007
[236] De Hert, P. (2005) Balancing security and liberty within the European Human Rights framework, *Utrecht Law Review*, vol. 1, no. 1, pp. 68-96
[237] Tyrer v. The United Kingdom, ECHR application no. 5856/72, 25 April 1978, para. 31; Dudgeon v. The United Kingdom, ECHR application no. 7525/76, 24 February 1983, para. 60; Soering v. The United Kingdom, ECHR application no. 14038/88, 7 July 1989, para. 102
[238] Von Hannover v. Germany, ECHR application no. 59320/00, 24 June 2004, para. 57
[239] Bygrave, L.A. (1998) Data protection pursuant to the right to privacy in human rights treaties, in *International Journal of Law and Information Technology*, vol. 6, pp. 247-284

horizontal context.[240] The applicable principles for both the positive and the negative obligation of the State are the same.[241]

In its case law the ECtHR held that the object of Article 8 ECHR "*is essentially that of protecting the individual against arbitrary interference by the public authorities*" and that "*in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for family life*".[242] In determining whether or not a positive obligation exists, a fair balance must be struck between the general interest of the community and the interest of the individual.[243] In order to avoid having an illusory and merely theoretically protected fundamental right, the State must make all the necessary positive arrangements to guarantee its effectiveness, in particular in relation to interferences by other private individuals.[244] If not the interference with the private life of the individual is considered as disproportionate and debited to the State. Although the object of Article 8 ECHR is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative obligation, there must be positive obligations inherent in an effective respect for private or family life.[245] They can require positive measures to be taken regarding the sphere of relations between individuals.[246]

3.2.1 The application of article 8 ECHR test by the ECtHR

The right to privacy as established in article 8 ECHR is not an absolute right.[247] The second paragraph of the article enlists the limits for its application. According to this provision, interference from public authorities with the private life and the correspondence of individuals is possible if it is done in accordance with the laws, is necessary in a democratic society and is counterbalanced by one of the following interests: national security, public safety, economic well-being of the country, prevention of disorder or crime, protection of health or morals, or the protection of rights and freedoms of

[240] X and Y v. the Netherlands, ECHR application no. 8978/80, 26 March 1985, para. 23

[241] Keegan v. Ireland, ECHR application 16969/90, 26 May 1994, para. 49; Botta v. Italy, ECHR application 21439/93, 24 February 1998, para. 33

[242] Marckx v. Belgium, ECHR application no. 6833/74, 13 June 1979, para. 31

[243] Rees v. The United Kingdom, ECHR application no. 9532/81, 17 October 1986, paras. 35-37; Cossey v. The United Kingdom, ECHR application no. 10843/84, 27 September 1990; paras. 36-37

[244] Marckx v. Belgium, ECHR application no. 6833/74, 13 June 1979, para. 31; X & Y v. The Netherlands, ECHR application no. 8978/80, 26 March 1985, para. 23; Gaskin v. The United Kingdom, ECHR application no. 10454/83, 7 July 1989, paras. 42-49

[245] Airey v. Ireland, ECHR application no. 6289/73, 9 October 1979, para. 32

[246] Eissen, M. (1993), The proportionality principle in the case law of the European court of Human Rights, in Macdonald, R.St.J., Matscher, F. and Petzold, H. (eds.), *The European System for the Protection of Human Rights*, pp. 125-137

[247] Kleining, P., et al. (2011), Security and Privacy: Global standards for ethical identity management in contemporary liberal democratic states, ANU E Press, p.43; Kilkelly, U. (2001), The right to respect for private and family life, Handbook no. 1, available online at: http://echr.coe.int/NR/rdonlyres/77A6BD48-CD95-4CFF-BAB4-ECB974C5BD15/0/DG2ENHRHAND012003.pdf (last check: 31.1.2013), p.6; Himma, K.E. (2007), Privacy vs. Security: Why privacy is not an absolute value or right, *San Diego Law Review*, vol. 45

others. As a result article 8 ECHR is not protecting the individuals against all interferences by the State, but only against those interferences that would qualify as arbitrary.

Even if in article 8 ECHR there is not an explicit separation between the right to privacy and the one to data protection, as it is now the case in the Charter of Fundamental Rights of the EU,[248] the ECtHR has been implicitly making such a distinction in its decisions. For the ECtHR, the mere collecting and storing of information (personal data) relating to an individual's private life by a public authority amounts in itself to an interference with the right to privacy. For this qualification, it does not matter if the data has been subsequently used or the way in which this was done.[249]

The ECtHR has further elaborated upon the criteria that qualify the nature of a State interference and has established a three-step test to evaluate: (a) the presence of interference by a public authority; (b) the legality of the interference; and (c) the necessity of the interference. The test is briefly discussed below.

First step: Interference by a public authority with the private life of the individuals

When dealing with claims for violation of article 8 ECHR, the ECtHR first establishes if there has been interference by a public authority with the rights of the individuals. The ECtHR has applied the provision broadly, covering not only cases in which there is evidence that an individual has been subject to interference, but also cases where such evidence is not present but there is a reasonable likelihood that this might have been the case.[250] For the ECtHR, the existence of legislation allowing secret surveillance measures amounts in itself to an interference with the applicant's rights under article 8 ECHR.[251] This broad interpretation is important for the protection of individuals since it is in most of the cases quite difficult, if not impossible, for an individual to prove that he has been subject to secret surveillance or untargeted surveillance by the State.

[248] See articles 7 and 8 of the Charter of Fundamental Rights of the EU; De Hert, P., Gutwirth, S. (2009), Data protection in the case law of Strasbourg and Luxembourg: Costitutionalisation in action, in Gutwirth at al. (eds), *Reinventing data protection?*, Springer, pp. 3-44

[249] Leander v. Sweden, ECHR application no. 9248/81, 26 March 1987, para. 48; Kopp v. Switzerland, ECHR application no. 23224/94, 25 March 1998, para. 53, Amann v. Switzerland, ECHR application no. 27798/95, 16 February 2000, para. 69

[250] Halford v. The United Kingdom, ECHR application no. 20605/92, 25 June 1997, para 56; Kennedy v. The United Kingdom, ECHR application no. 26839/05, 18 May 2010, para. 124; De Hert, P. (2005), Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, vol. 1, issue 1, pp. 68-96

[251] Klass v. Germany, ECHR application no. 5029/71, 6 September 1978, para. 34; Iordachi v. Moldavia, ECHR application no. 25198/02, 10 February 2009, para. 33

Also cases in which the public authorities have not been involved directly in the interference with the private life of the individuals fall under Article 8 ECHR.[252] This would be the case if, for example, a communication is intercepted by one of its participants, on its own initiative, while the authorities have been informed. For the ECtHR, the consent from one of the parties to the recording does not change the private character of a conversation.[253] In addition the ECtHR is aware that such practices might be dangerously infringing the rights of individuals if the authorities have the possibility to evade legal obligations by making use of private agents.[254] Therefore these situations are considered as State interference and will fall under the prohibition of the first paragraph of Article 8 ECHR.

Second step: The legality requirement

In this step the ECtHR focuses on the legality requirement. The explanation of the ECtHR of the article 8 ECHR wording "*in accordance with the law*" is followed by a number of requirements.[255] On one side the notion of law implies qualitative requirements, notably those of accessibility,[256] foreseeability,[257] and compatibility with the rule of law.[258] On the other side, the ECtHR uses an extensive interpretation of the term "law", not limiting it to what is being formally considered as such, but giving to it a substantive meaning, comprising the written as well as the unwritten law.[259] The ECtHR explicitly refers to the phenomenon of perpetual technological change, as an argument to accept unwritten law as a legal ground for human rights limitations.[260]

Targeted interception of communications without a mandate and outside a legal process cannot be justified under the second paragraph of article 8 ECHR.[261] In *Malone* the ECtHR ruled that wiretapping without clear legal guidelines amounts to an infringement of the right to privacy.[262] For the ECtHR, States that are members of the ECHR may not, in the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. They have first to consider the consequences that these measures might have for the protection of the fundamental rights of the individuals in a democratic society.[263]

---

[252] M.M. v. The Netherlands, ECHR application no. 39339/98, 8 April 2003, para. 42; A. v. France, ECHR application no. 14838/89, 23 November 1993, paras. 38-39

[253] A. v. France, ECHR application no. 14838/89, 23 November 1993, para. 36

[254] Van Vondel v. The Netherlands, ECHR application no. 38258/03, 25 October 2007, para. 49

[255] Kopp v. Switzerland, ECHR application no. 23224/94, 25 March 1998, para. 55; Perry v. The United Kingdom, ECHR application no. 63737/00, 17 July 2003, para. 55; Taylor, N. (2001) State surveillance and the right to privacy, in *Surveillance and Society*, Vol. 1, no. 1, pp. 66-85

[256] Khan v. The United Kingdom, ECHR application no. 35394/97, 12 May 2000, para. 27

[257] Huvig v. France, ECHR application no. 11105/84, 24 April 1990, para. 26

[258] Huvig v. France, ECHR application no. 11105/84, 24 April 1990, para. 34; Moonen, T. (2010), Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights, Pace Int'l L. Rev. Online Companion, pp. 97-142

[259] Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 35; Huvig v. France, ECHR application no. 11105/84, 24 April 1990, para. 34

[260] Huvig v. France, ECHR application no. 11105/84, 24 April 1990, para. 28

[261] M.M. v. The Netherlands, ECHR application no. 39339/98, 8 April 2003, para. 45

[262] Malone v. The United Kingdom, ECHR application no. 8691/79, 2 August 1984, paras. 67-68

[263] Klass v. Germany, ECHR application no. 5029/71, 6 September 1978, para. 48

The evaluation changes in cases of untargeted surveillance, for which it is impossible to ask for an individual mandate. The ECtHR extended the application of article 8 ECHR and of the test it has established for cases of individual surveillance also to cases of mass surveillance. For the ECtHR there are no grounds to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.[264] Since in most of the cases it is impossible for an individual to know or prove the fact that his private life has been interfered via mass surveillance measures, the ECtHR accepts complaints also from individuals that cannot prove to have been individually subject to such surveillance practices. In these cases, the individuals may challenge the national legislation which allows a system of mass surveillance.[265]

For the ECtHR it is necessary however that States have clear and detailed rules, especially since the technology available for surveillance is continuously becoming more sophisticated.[266] In *Marper* the ECtHR clearly showed that the protection afforded by article 8 ECHR would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system was allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.[267] Even if the *Marper* case falls in the area of retention of finger prints and DNA samples, the reasoning of the ECtHR can be extended to all the areas covered by the protection of article 8 ECHR. The reasoning is thus relevant also for cases of surveillance with non-purpose built technology.

Third step: Necessity criteria

Even in the presence of a measure interfering with the privacy of the individuals, that is based on the law and serves an objective listed in article 8(2) ECHR, the ECtHR would check in the third step of the test if such a measure can be considered as "necessary in a democratic society". The resulting interference with the private life of an individual can only be regarded as "necessary in a democratic society" if the particular system of surveillance adopted contains adequate guarantees against abuse from the public authorities.[268]

The phrase "necessary in a democratic society" has not been receiving a clear interpretation from the ECtHR. In *Handyside*[269] the ECtHR held that while the adjective necessary is not synonym with indispensable, it has neither the flexibility of such expressions as: admissible, ordinary, useful,

[264] Liberty and Others v. The United Kingdom, ECHR application no. 58243/00, 1 July 2008, para. 63
[265] Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 78
[266] Huvig v. France, ECHR application no. 11105/84, 24 April 1990, para. 32
[267] S. and Marper v. The United Kingdom, ECHR applications no. 30562/04 and 30566/04, 4 December 2008, para. 112
[268] Malone v. The United Kingdom, ECHR application no. 8691/79, 2 August 1984, para. 81
[269] Handyside v. United Kingdom, ECHR application no. 5493/72, 7 December 1976, para. 48

reasonable or desirable. With this phrase it is understood that the interfering measure must correspond to a "pressing social need" (which is also not defined!) and must be proportionate to the legitimate aid pursued.[270] The fact that the ECtHR avoids to give a definition of what has to be considered as "necessary in a democratic society" is related with the margin of appreciation doctrine. The ECtHR holds that the exclusivity to interpret and apply national law to domestic situations[271] should remain within the domain of national authorities.[272] This approach becomes even stronger in cases of measures introduced with the scope of protecting national interests. In such situations, it has been reiterated that it is for the national authorities to judge what is necessary in order to protect the domestic interests. The attention of the ECtHR in such cases is focused on the analyses of the legal safeguards and guaranties offered to the individuals.[273] This is also related, of course with the separation of powers between the legislative and the judiciary. The ECtHR takes only a marginal view of the application of the principle when there is discretion to decide for national authorities.[274] It is difficult for the courts at national as well as at international level to evaluate a decision taken by national authorities to which the legislator, apart the competence for deciding, has been leaving also a margin of appreciation for deciding or a decision taken from the legislator itself.

3.2.2 Concluding remarks

Article 8 ECHR protects the right to privacy of individuals even though, in the absence of a conclusive definition of the right, a case by case assessment is needed for establishing if a situation falls within the scope of the article. This protection is vertical, against arbitrary State interventions even though the ECtHR has clarified that the State has both a negative and a positive obligation for protecting the right of the citizens.[275] When new technology is used for interfering with the life of the citizens the ECtHR requires a careful balancing between the public benefits and the private life interests.[276] The lacking of such a balancing would weaken the protection of article 8.[277] The technology neutral fashion in which the article is written makes State interferences with the private life of the individuals both in situations of traditional surveillance and in situations of surveillance with non-purpose built technology fall within the scope of application of the article.

Even if the article was first directed towards targeted interference with the rights of the citizens, the ECtHR extended its application also to cases of mass surveillance.[278] In these cases one does not need

[270] Harris, D. et al. (2009), Law of the European Convention on Human Rights, Oxford University Press, second edition, p. 349
[271] Arai-Takahashi, Y. (2002), The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR, Intersentia, p. 14
[272] Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 29; M.K. v. France, ECHR application 19522/09, 18 April 2013, para. 43
[273] Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 106; Klass v. Germany, ECHR application no. 5029/71, 6 September 1978, para. 50
[274] Jans, J.H. et al. (2007), Europeanisation of Public Law, Europa Law Publishing, p. 151
[275] Von Hannover v. Germany, ECHR application no. 59320/00, 24 June 2004, para. 57
[276] Klass v. Germany, ECHR application no. 5029/71, 6 September 1978, para. 48
[277] S. and Marper v. The United Kingdom, ECHR applications no. 30562/04 and 30566/04, 4 December 2008, para. 112
[278] Liberty and Others v. The United Kingdom, ECHR application no. 58243/00, 1 July 2008, para. 68

to prove to have been individually subject of such surveillance but still has the right to challenge the existing rules that introduce such a form of surveillance. In situations in which the measures are introduced for the scope of national security the protection is however weak. Due to the margin of discretion enjoyed by national authorities the attention of the ECtHR in such cases is limited to the existence of legal safeguards and guarantees. With regards to incidental surveillance and retroactive surveillance, as already discussed in chapter 2, section 3, the case law from the ECtHR does not protect the rights of individuals that find themselves in such situations.

3.3 Other legal instruments at Council of Europe level - The emergence of the right to "data protection"

Following the discussion of the interpretation of the right to a protected private life in article 8 ECHR, the present sub-section will focus on the introduction of other legal instruments at the Council of Europe level. The introduction of these legal instruments is closely linked with the emergence of the right to data protection. The development of this right for the Council of Europe will therefore be presented and the principles for protecting the privacy of the individuals in cases of surveillance by the State will be discussed.

3.3.1 Convention 108

Protection of personal data was not originally discussed in the Council of Europe framework, but development of technology and increased exposure of personal information from individuals raised the awareness that the right to privacy as laid down in article 8 ECHR had certain limitations. It was becoming evident that effective legal protection of personal data would require more specific and systematic approach than the general reference to respect for private life in article 8 ECHR. "…*the scope of the right was uncertain, and in any case did not cover all personal information; it was mainly directed against public authorities, even though private sector organisations could also create privacy risks through the use of large databases; and finally, it was felt that a comprehensive and more proactive approach was necessary in view of the challenges of an information society already visible on the horizon*."[279]

These concerns[280] led to the adoption of Convention 108 for the protection of individuals with regard to automatic processing of personal data (Convention 108) where the term "data protection" emerged.[281] In Convention 108 the term "data protection" was linked with the protection of fundamental rights and freedoms of natural persons, in particular of their right to privacy, with

[279] Hustnix, P. (2014) The reform of EU data protection: towards more effective and more consistent data protection across the EU, in Witzleb, N., Lindsay, D., Paterson, M., Rodrick, S. (eds.), Emerging challenges in Privacy law, Cambridge University Press, pp. 62-71

[280] Bygrave, L. (2008) International agreements to protect personal data, in Rule, J. B., Greenleaf, G. (eds.), Global privacy protection, Edward Elgar, p. 20

[281] Convention for the protection of individuals with regard to automatic processing of personal data, No. 108, 28 January 1981

respect to the processing of personal data.[282] This definition shows very clearly the way data protection was seen to interlink with the right to privacy. There is an undeniable close relationship between both rights.[283] They are closely related, partly overlapping, but also indicating the possibility that data protection is separated from the right to privacy in those situations in which data protection will serve for the protection of other fundamental rights than privacy.

Convention 108 requests the signatory parties to apply the principles that are laid down in its provisions to ensure the respect for fundamental rights with regard to processing of personal data. The data protection principles identified[284] in this Convention are:

a. principle of lawfulness of processing;
b. principle of finality/purpose;
c. principle of proportionality;
d. principle of the length of conservation;
e. principle of transparency;
f. right of access;
g. principle of quality of data: right of rectification and erasure;
h. principle of independent supervision;
i. principle on security measures.

These different principles aim at the fulfilment of two fundamental legal standards. Firstly, the personal data collected should be correct, relevant and not excessive in relation to their purpose. Secondly, their use (gathering, storage, dissemination) should likewise be lawful. If personal data are managed in conformity with these principles, there is no arbitrary interference with the protected private life of the individuals that would derive from them.

Convention 108 applies both for the private as well as for the public sector.[285] Also law enforcement and national security bodies fall under the provisions of this Convention as well as judicial authorities. For the latter, in a report of 2002[286] the Council of Europe found that even if Member States party to the Convention 108 have not implemented directly the data protection principles contained therein, there are other national rules that, even if not specifically designed with data protection in mind, have the same effects as data protection principles. An example would be the national criminal procedural rules that include safeguards for accused persons, rules for collecting evidence, balance of interest in a fair trial, etc. In this light, one can see that in a Council of Europe context not only the right to data protection was not introduced as a separate right from the one to privacy but also that the principles related with it were not originally designed for the protection of

[282] Article 1 Convention 108
[283] Verhey, L. (2014) Privacy in the Dutch Constitution: a dead letter?, in Hijmans, H., Kranenborg, H. (eds.), *Data protection anno 2014: How to restore trust?*, Intersentia, pp. 69-81
[284] Article 5 Convention 108
[285] Article 3(1) Convention 108
[286] Council of Europe (2002) Report on the impact of data protection principles on judicial data in criminal matters including in the framework of judicial co-operation in criminal matters

this right. The data protection principles were identified from the existing legal principles of the national legislation. The European Communities asked to access Convention 108 in 1997[287] but as of today, not all the formal requirements are met for this accession.[288] Since Convention 108 is written in a technology neutral fashion, it has the possibility to cover situations of surveillance with non-purpose built technology.

The European Court of Human Rights does not have jurisdiction on Convention 108, meaning that it is not possible to start a procedure before this Court on the basis of the provisions of such Convention. Despite this, Convention 108 is a legally binding international instrument.[289] With regards to data protection the ECtHR has established in its case law its own definition. The elaboration of the ECtHR has been however closely linked with the legislative developments and influenced by them. Data protection is seen in the case law as one aspect of the right to a protected private life and not as a separate right. The close relationship between protection of private life and data protection is established in the framework of the Human Rights Convention. This aspect was clearly stated in the case *M.S. v. Sweden* of 27 August 1997[290] in which the ECtHR reiterated that "*the protection of personal data (..) is of fundamental importance to a persons' enjoyment of his or her right to respect for private and family life as guaranteed by article 8 of the Convention*".

Also access to personal data has been considered by the ECtHR as falling within the scope of article 8 ECHR. In an earlier decision, in *Gaskin*[291] the ECtHR held that the lack of access to files related with the childhood of the applicant is not in conformity with article 8 ECHR. The right to access the data gives also the possibility to individuals to ensure the accuracy of the data as well as that they have not been collected and processed in an illegal manner.[292]

In a number of other judgments the ECtHR has been focusing on the justifications of the interference with the private life. For example, in *S. and Marper v. the United Kingdom*[293] the ECtHR held that the blanket and indiscriminate retention of personal data constitutes a disproportionate interference

[287] Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede adopted by the Council of Ministers, in Strasbourg 15 June 1999

[288] Art. 21(6) of the Convention 108 provides that the amendments will come into force on the 30th day after all parties to the Convention have accepted them. So far only 36 out of 42 parties have accepted.

[289] Greenleaf, G. (2014) A world data privacy treaty? 'Globalisation' and 'modernization' of Council of Europe Convention 108, in Witzleb, N., Lindsay, D., Paterson, M., Rodrick, S. (eds.), *Emerging challenges in Privacy law*, Cambridge University Press, pp. 93-138

[290] M.S. v. Sweden, ECHR application 20837/92, 27 August 1997, para. 41; see also Z. v. Finland, ECHR application 22009/93, 25 February 1997, para. 95

[291] Gaskin v. The United Kingdom, ECHR application no. 10454/83, 7 July 1989, para. 42-49; in the same line see also the decision in Marckx v. Belgium, ECHR application no. 6833/74, 13 June 1979, para. 31

[292] Khelili v. Sweden, ECHR application no. 16188/07, 18 October 2011, para. 64; see also Fink, U. (2014) Protection of privacy in the EU, individual rights and legal instruments, in Witzleb, N., Lindsay, D., Paterson, M., Rodrick, S. (eds.), *Emerging challenges in Privacy law*, Cambridge University Press, pp. 75-91

[293] S. and Marper v. the United Kingdom, ECHR application nos. 30562/04 and 30566/04, 4 December 2008, paras. 119-125

with the applicants' right to respect for private life. In *B.B. v. France*[294] the national law was found to have sufficient data protection safeguards, the data subject could request erasure, the data storage had a limited length and access and a fair balance was struck between the competing private and public interest at stake.

From the above elaboration, it can be concluded that originally, in a Council of Europe context, the right of data protection departed from the right to privacy to ensure a better protection of the latter when personal data of individuals were concerned, especially with the computerization and technological developments of the society. This close relationship of the two rights can be identified both in the legal documents adopted by the organs of the Council of Europe as well as in the decisions of the European Court of Human Rights. Data protection is considered as incorporated in the provision of article 8 ECHR.

3.3.2 Non-binding instruments

In light of the Convention 108, a number of non-binding legal instruments directed to the Council of Europe Member States have been adopted. These instruments reiterate the data protection principles identified in Convention 108 and cover processing of personal data in different sectors as for example health, insurance, police, etc.[295]

While the first non-binding legal instruments adopted at the Council of Europe were based on Convention 108 the latter ones refer to human rights principles in general.[296] The non-binding nature of the adopted legal instruments weakens, however, the applicability of the data protection

[294] B.B. v. France, ECHR application no. 5335/06, 17 December 2009, para. 61

[295] Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling; Recommendation No. R (2002) 9 on the protection of personal data collected and processed for insurance purposes; Recommendation No. R (99) 5 on the protection of privacy on the Internet; Recommendation No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes; Recommendation No. R (97) 5 on the protection of medical data; Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services; Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies; Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations; Recommendation No. R (89) 2 on the protection of personal data used for employment purposes; Recommendation No. R (87) 15 regulating the use of personal data in the police sector; Recommendation No. R (86) 1 on the protection of personal data used for social security purposes; Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing; Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics

[296] Recommendation CM/Rec(2012)3 of the Committee of Ministers to member states on the protection of human rights with regard to search engines; Recommendation CM/Rec(2012)4 of the Committee of ministers to member states on the protection of human rights with regard to social networking services; Recommendation Rec(2007)1 of the Committee of Ministers to member states on co-operation against terrorism between the Council of Europe and its member states, and the International Criminal Police Organisation (ICPO - Interpol); Declaration of the committee of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies (adopted on 11 June 2013)

principles for the Member States. The importance of these non-binding legal instruments is in the way data protection and privacy are considered and interlink at the Council of Europe level were, even if non-binding, the documents show the will of the Member States and have influenced their national legislation. Thus, in the following sub-section these instruments are not discussed one by one but the principles contained in them and that are relevant for the protection of the right to privacy and personal data of the individuals are extracted.

3.3.2.1 The principles for protecting privacy and personal data in non-binding legal instruments of the Council of Europe

This sub-section presents relevant principles for the protection of the private life of the individuals from interference by States via surveillance measures identified in non-binding instruments at Council of Europe level. These legal instruments are mainly technology neutral as to give the possibility to cover in the future also new technologies developed and used to interfere with the rights of individuals. As such they apply also in cases of surveillance with non-purpose built technology.

These legal instruments cover also the law enforcement sector and will apply when interference with the private life of the individuals qualifies as State surveillance. Because of the historical evolution of the rights, the legislator has not made thus far a clear distinction between interferences with the private life of the individual and the personal data. Data protection is considered as one of the aspects of the right to privacy and covered by article 8 ECHR. The absence of case law from the ECtHR on Convention 108 and on other non-binding legal instruments at Council of Europe level raises the question if these legal instruments have been extending the right contained in article 8 ECHR to apply also in horizontal situations – when for example there is interference with the right to privacy of the individual as a result of processing of personal data from other private parties. An argument against this reasoning is that data protection principles for safeguarding the privacy of individuals in horizontal situations are only a manifestation of how Member States should react for fulfilling their positive obligation under article 8 ECHR.[297] The current distinction of the two rights in the European Union might also talk for the lack of intention of the legislator to extend the right to privacy to horizontal situations. This will be further discussed in the following section.

The identified principles address various aspects of the interference with the private life of the individuals, as for example in the case of profiling, the use of communication services, criminal investigations, etc. With regards to profiling[298] it is stated that collection and processing of personal data should be fair, lawful and proportionate, and for specific and legitimate purposes.[299] The personal data should be relevant, adequate and not excessive in relation to the reasons for which

[297] Von Hannover v. Germany, ECHR application no. 59320/00, 24 June 2004, para. 57
[298] Recommendation of the Council of Ministers Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling
[299] Rec(2010)13, para. 3.1

they are collected and processed.[300] The data subject can be identified only for as long as it is necessary for the purpose of data collection[301] and the collection and processing can be done only if provided by law, or permitted by law and there is the consent of the data subject.[302] But in situations of necessity in a democratic society the Member States are not obliged to apply the abovementioned safeguards when this is provided by law.[303] The exceptional situations cover: State security, public safety, monetary interests of the state, prevention or suppression of criminal offences, protecting the data subject or the rights and freedoms of others.

With regards to telecommunication services and in particular telephone services a distinction exists between the content of the communication including the use of listening or tapping devices or other means of interception of communications, and other metadata collected and processed by network operators. However, the level of legal safeguards required is the same for both types of data.[304] This identical standard shows that the fact that certain data are more easily obtained and are exposed to third parties, as it is the case of the service providers, does not make them a second-class data less worthy of protection. Interference of public authorities with the content of a communication as well as with other personal data collected by operators must be carried out only when provided by law and constitutes a necessary measure in a democratic society.[305] As seen above, also the situations in which the interference can take place are clearly identified: protecting state security, public safety, monetary interests of the State, suppression of criminal offences, and protecting the data subject or the rights and freedoms of others. The focus of the legislator on the aspects of private life that are interfered with (e.g. communications) instead of the technology used can be seen very clearly in the area of telecommunication as well.

In the Guidelines of the Council of Ministers on human rights and the fight against terrorism,[306] a distinction is made between interference with personal data (collection and processing) and the private life of the individuals.[307] Collection and processing of personal data is considered as interfering with the private life only if it fails a number of safeguards: (i) it is not governed by appropriate provisions of domestic law; (ii) it is not proportionate to the aim for which the collection and processing was foreseen; (iii) it is not subject to supervision by an external independent authority. If these safeguards are instead fulfilled, then the interference with the personal data is lawful for the rules designed for the protection of the right to privacy. With regard to other measures that are considered to interfere with the right to privacy but that are not qualified as an interference with personal data, it is required that they are provided by law and have the possibility to be

[300] Rec(2010)13, para. 3.2
[301] Rec(2010)13, para. 3.3
[302] Rec(2010)13, para. 3.4
[303] Rec(2010)13, para. 6
[304] Recommendation no. Rec(95)4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services
[305] Rec(1995)4, paras. 2.4 and 4.2
[306] Guidelines of the Committee of Ministers of the CoE on human rights and the fight against terrorism, 11 July 2002
[307] Guidelines of the Committee of Ministers of the CoE on human rights and the fight against terrorism, 11 July 2002, paras. v and vi

challenged before a court. Possible derogations to such rules are allowed when the fight against terrorism takes place in a situation of war or public emergency which threatens the life of the nation. Such derogations must however go only to the extent strictly required by the exigencies of the situation, and the derogations must remain within the limits and conditions fixed by international law.[308]

With regards to the collection of personal data from the police authorities[309] it is required that this is limited to the prevention of a real danger or the suppression of a specific criminal offence. This requirement would imply that untargeted surveillance of citizens, done for the prevention of potential future dangers, is considered as not in conformity with the human rights principles. As a result, the Member States are recommended to rule it out.[310] Also in the European Code of Police Ethics[311] it is stated that the police: "*shall only interfere with individual's right to privacy when strictly necessary and only to the extent required to obtain a legitimate objective".*[312] This formulation implies not only the need of legal provisions on the basis of police operations, but also that arbitrary interferences are not accepted. Furthermore, it indicates that interference with the right to privacy must always be considered as an exceptional measure and, even when justified, should involve no more interference with the individual's life than is absolutely necessary (in conformity with the proportionality principle).

The use of new information technologies largely facilitates police action against different forms of criminality. The registration and the analysis of personal data, in particular, allows the police to cross-check information and thus to expose networks whose existence would otherwise remain obscure without resort to these tools. However, the uncontrolled use of personal data may constitute violations of the right to privacy of the individual concerned. In order to avoid abuse at the stages of collection, storage and use of personal data, such police activities must be guided by the data protection principles.[313]

Special investigation techniques, i.e. techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the targeted persons,[314] should be allowed only when there are sufficient reasons to believe that a serious crime has been committed or prepared, by one or more particular persons or as yet unidentified individual or group of individuals.

[308] Guidelines of the Committee of Ministers of the CoE on human rights and the fight against terrorism, 11 July 2002, para. xv

[309] Recommendation no. R(87)15 regulating the use of personal data in the police sector

[310] However, a different approach is taken by the European Court of Human Rights as discussed in the Klass v. Germany case

[311] Recommendation Rec(2001)10 adopted by the Committee of Ministers of the Council of Europe on 19 September 2001

[312] Rec(2001)10, para. 41

[313] Rec(2001)10, para. 42

[314] Recommendation R(2005)10 of the Committee of Ministers to Member States on "special investigation techniques" in relation to serious crimes including acts of terrorism

When deciding on their use, the proportionality between the effects of the use of special investigation techniques and the objective that has been identified must be insured. These techniques are therefore suggested to be used for the detection or prevention of specific crimes and not for situations of untargeted surveillance such as, for example, mass surveillance.

Lately the Council of Europe has been more aware on the development of technology and its role for interfering with the private life of the individuals. As a result, technology is more present in recent Council of Europe documents. An example of such an approach is the Declaration of the Council of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies.[315] Also for those situations the Member States attention is directed to the relevant Council of Europe standards on privacy and data protection, the 1966 United Nations International Covenant on Civil and Political Rights,[316] other international human rights instruments as well as the principle of proportionality. Other examples were technology is direct part of the concern of the Council of Europe are the Recommendations on search engines[317] and the use of internet.[318] The need to comply with article 8 ECHR and the Convention 108 principles is expressively stated in these situations. It is recognized that the use of internet, as a public service, and especially of the search engines create the possibility to generate new kinds of personal data, such as individual search histories and behaviour profiles.

3.3.3 Concluding remarks

The aim of this section was to identify other legal instruments than the European Convention of Human Rights provided by the Council of Europe for the protection of the right to privacy of European Citizens in the presence of State surveillance. Apart Convention 108 on automatic processing of personal data also a number of non-binding legal instruments were identified. Even though non-binding these instruments guide and influence the national legislation of the Member States and contain a number of principles to be used for the protection of the right to privacy of citizens.

Council of Europe legal instruments cover interferences by law enforcement and national security bodies alike. Their focus is not on the technology used for interfering with the private sphere of the individuals but on the way this is done. This technology neutrality of the laws allows the extension of the application of the provisions to the new technology used for surveillance and to non-purpose built technology.

[315] Declaration of the Council of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies, 11 June 2013
[316] International Covenant on Civil and Political Rights (ICCPR) adopted by the United Nations General Assembly on 16 December 1966
[317] Rec(2012)3 of the Council of Ministers to the Member States on the protection of human rights with regards to search engines
[318] Recommendation CM/Rec(2007)16 of the Committee of Ministers to Member States on measures to promote the public service value of the Internet

While no special attention is paid to the surveillance technology, data protection is seen as closely linked with the right to privacy and the identified legal instruments suggest that all law enforcement activities must be guided by the data protection principles for complying with the protection of the right to privacy. In addition, on the basis of these non-binding legal instruments, interferences with the privacy of the individuals should not go further than what it is strictly necessary, metadata should enjoy the same level of protection as content data and special investigation techniques must be limited only to clearly identified cases. These principles are relevant also for surveillance with non-purpose built technology, though it must be added that the special challenges that this form of surveillance creates for the protection of the right to privacy (namely: incidental surveillance, mass surveillance and retroactive surveillance) are not addressed.

3.4 The Charter of Fundamental Rights of the EU - The separation of the rights to privacy and data protection

After discussing the development of the right to a protected private life in a Council of Europe context and identifying the relevant principles designed for the protection of this right from State interferences, the chapter will continue with the elaboration of the relevant EU legislation. The present section will focus on the Charter of Fundamental Rights of the EU (the Charter). The Charter presents the right to privacy as separate from the one to data protection. The nature of the rights is discussed in light of the case law from the European Court of Justice as well as of the doctrine. The clarification of the links between the two rights is important for this research since it gives the possibility to assess in how far the legislation designed for the protection of personal data does protect the right to privacy of the individuals from State surveillance.

From their creation in 1951, the European Communities focused on furthering the economic development of the Member States and creating such interdependence between them that would make future wars "*not only unthinkable but also impossible*".[319] The protection of the fundamental rights of the citizens was at the beginning not part of the fields in which the Communities were operating.[320] This gap in the application of the fundamental rights was filled with a number of decisions from the European Court of Justice. Already in 1969 in *Stauder*[321] the CJEU ruled that fundamental human rights are general principles of law to be protected in the Communities and that legal instruments adopted at Community level had to comply with them. In the subsequent case law it was clarified that in deciding which fundamental rights will be part of the general principles of Community law the CJEU drew inspiration from the constitutional traditions common to the Member

[319] The Schumann Declaration proposing the creation of the Coal and Steel Community was presented by French foreign minister Robert Schuman on 9 May 1950

[320] This might be related also with the fact that the projects for a Political Community and a Defence Community to operate alongside the Economic Community were not successful.

[321] Case 29/69 Stauder [1969] ECR 419, para. 7

States as well as to international treaties to which the Member States were parties – the European Convention of Human Rights being the most important among them.[322]

Fundamental rights as general principles of law were to apply first of all towards acts of the Community institutions themselves[323] and then towards the Member States.[324] The European Community, however, could not become a member of the European Convention of Human Rights, even if all its Member States were already part of it.[325] Also a current attempt to draft an agreement for the accession of the EU at the ECHR after the Treaty of Lisbon gave this competence to the Union was evaluated by the CJEU as unsuccessful since it did not take into account the special nature of the EU as a supranational organisation.[326] This inability brought the initial ideas for adopting a human rights document that was binding for the Union[327] and its Member States.[328] As a result, the Charter of Fundamental Rights of the European Union was first proclaimed at Nice on 7 December 2000.[329] The Charter did not have originally any binding value. The legal status of the Charter was later clarified by the Lisbon Treaty and nowadays, on the basis of article 6(1) TEU it has the same legal value as the other EU Treaties.[330] The Charter applies in vertical relationships.[331] Its provisions are addressed to Union institutions and bodies and to the Member States in as far as they operate in the field of application of EU law.[332]

The Charter distinguishes the right to a protected private life (article 7)[333] from data protection which is presented as an explicitly separate right in the following article (article 8).[334] The formulation of

[322] Case 11/70 Internationale Handelsgesellschaft [1970] ECR 1125, para. 4; Case 4/73 Nold [1974] ECR 491, para. 13; Case C-260/89 Elliniki Radiophonia Tileorassi AE (ERT) v. Dimotiki Etairia Pliroforissis [1991] ECR I-2925, para. 41

[323] Joined cases C-402/05P and C-415/05P Kadi and Al Barakaat v. Council [2008] ECR I-6351, para. 285

[324] Case C-60/00 Carpenter [2002] ECR I-6279, para. 41

[325] Opinion 2/94 on Accession by the Community to the ECHR [1996] ECR I-1759

[326] Opinion 2/13 of the Court on the accession of the EU in the ECHR EU:C:2014:238, para. 2454

[327] The European Union was created in 1993 with the entry into force of the Maastricht Treaty, see Article A

[328] Anderson, D., Murphy, C. (2011) The Charter of Fundamental Rights: History and prospects in post-Lisbon Europe, in *EUI Working papers*, August 2011

[329] Charter of Fundamental Rights of the European Union, OJ [2000] C364/1

[330] Spaventa, E. (2014) Fundamental Rights in the European Union, in Barnard, C., Peers, S. (eds.), *European Union Law*, OUP, pp. 226-254

[331] Article 51 of the Charter

[332] C-617/10 Aklagaren v. Hans Akerberg Fransson EU:C:2013:280, para. 21; Case C-390/12 Pfleger et al. EU:C:2014:281, para. 36

[333] Article 7 of the Charter:

"*Respect for private and family life*

Everyone has the right to respect for his or her private and family life, home and communications."

[334] Article 8 of the Charter:

"Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

article 7 of the Charter resembles the one of the first paragraph of article 8 ECHR. A provision similar with the second paragraph of article 8 ECHR, that expresses the not absolute nature of the right to a protected private life, can be found in article 52(1) of the Charter. Limitations to the right are exceptionally allowed if provided by law and respect the essence of the right. Such limitations must be necessary and proportionate and meet objectives of general interest or the need to protect the rights and freedoms of others. The EU has, however, never conclusively defined the right to privacy.[335]

The formulation of article 8 of the Charter is, on the other side, original and not to be found in other human rights conventions even though it is inspired by those.[336] It is difficult to decode the intention of the legislator when drafting this article since from the explanations relating to it the article results as simultaneously inspired by article 286 TEC, Directive 95/46/EC, article 8 ECHR and Convention 108.[337]

This expressed distinction between the two rights is a novelty but also an affirmation of doctrinal debates and a number of decisions from the European Court of Justice. It did, however, not close the existing debates on the nature of the rights since both in the doctrine as well as in court decisions the terms continue to be used interchangeably and thus the terminology is at times confusing. While all would agree that both rights are closely related, it is important at this point to clarify their links and interdependence to assess in how far the data protection legislation is covering also the protection of the right to privacy.

3.4.1 Privacy v. Data protection - The judicial and doctrinal debate

As it was seen in the previous section, in the European Convention of Human Rights only the right to a protected private life is explicitly mentioned. The right to data protection[338] was created afterwards as a specification of the right to privacy in the digital era by Convention 108 and the case law of the Court of Human Rights.[339] For the Council of Europe, data protection is still considered as part of the right to a protected private life and is covered by the extended interpretation of article 8 ECHR, even though it is agreed that data processing is broader than the interest not to interfere with ones'

[335] Bergkamp, L. (2002) EU data protection policy - The privacy fallacy: Adverse effects of Europe´s data protection policy in an information-driven economy, *Computer Law & Security Report*, vol. 18, no. 1, pp. 31 - 47
[336] De Schutter, O. et al. (2006) The Commentary of the Charter of Fundamental Rights of the European Union, available online at: http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf (last accessed: 2.5.2013), p. 90
[337] Explanations relating to the Charter of Fundamental Rights, OJ C 303/17, available online at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF (last accessed: 16.09.2016)
[338] For a historical view into the development of the right to data protection in the EU see: Mayer-Schoenberger, V. (1997) Generational development of data protection in Europe, in Agre, P.E., Rotenberg, M. (eds.), *Technology and Privacy: The new landscape*, pp. 219-238
[339] De Hert, P., Papakostantinou, V. (2013) Three scenarios for international governance of data privacy: Towards an international data privacy organisation, preferably a UN agency?, *A Journal of Law and Policy for the Information Society*, vol. 9, no. 2, pp. 271-324

private life. For example, in *Friedl*[340] the fact that someone was photographed in a manifestation by the police, but was not identified, was not considered as a violation of his right to a protected private life but it was still qualified as falling in the field of data protection. In general, it can be said that publicly available personal data which are not systematically collected or stored are considered as not interfering with the right to a protected private life. In this sub-section the attention is focused on the case law from the Court of Justice of the EU and the doctrinal debate on the topic.

According to Gutwirth and De Hert (2006),[341] there are 3 main differences that distinguish the nature of the right to privacy from the one to data protection. First of all, data protection explicitly protects values that are not at the core of privacy, such as for example the requirement of fair processing, consent or legitimacy. Secondly, the recognition of a separate right to data protection next to the right to privacy is more respectful to the different European constitutional traditions. Contrary to countries such as Belgium that have from the start linked data protection to privacy, countries such as France and Germany, have searched and found other legal anchors for the recognition of these rights.[342] Such a call from different Member States of the EU for separating the two rights was expressed also in the framework of the consultative meetings for modernising Convention 108.[343] And last, but not the least, since data protection has grown in response to problems generated by new technology,[344] and especially the increased use of computers, it would not bring any added value to reduce all these response to technology to just ´privacy´.[345]

Even if it is clear that data protection and privacy cannot be used as synonyms and not all personal data are by their nature capable of interfering with the private life of the individuals, a confusing and interchangeable use of both terms has been seen in the case law of the Court of Justice of the EU, especially before the entry into force of the Treaty of Lisbon.[346] In *Rundfunk*,[347] for example, the CJEU treated data protection and privacy as two interchangeable rights, reinforcing the belief that data protection was a subset of the right to privacy. The same appeared in *Lindqvist*.[348] In *Satamedia*,[349]

[340] Friedl v. Austria, ECHR application 15225/89, 31 January 1995
[341] Gutwirth, S., De Hert, P. (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, pp. 61-104
[342] Fuster Gonzales, G. (2014) The emergence of data protection as a fundamental right of the EU, Springer, p. 92
[343] Consultative Committee on the protection of individuals with regards to automatic processing of personal data (2012) (T-PD), p. 32
[344] Gonzalez Fuster, G. (2014) The emergence of data protection as a fundamental right of the EU, Springer, p. 86; Sloot, B., van der (2014) Privacy in the Post-NSA Era: Time for a Fundamental Revision?, *JIPITEC*, vol. 5, no. 2, available online at: https://www.jipitec.eu/issues/jipitec-5-1-2014/3901 (last accessed: 12.4.2016)
[345] Gutwirth, S., De Hert, P. (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, pp. 61-104
[346] De Hert, P., Gutwirth, S. (2009) Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action, in Gutwirth, S., Poullet, Y., De Hert, P., Nouwt, J. & De Terwangne, C. (eds), *Reinventing Data Protection?*, Springer, pp. 3-44
[347] Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-04989, para. 74
[348] Case 101/01 Lindqvist [2003] ECR I-12971, para. 86
[349] Case C-73/07 Satakunnan Markkinapörssi and Satamedia [2008] ECR I-09831, para. 55

Directive 95/46[350] on the protection of personal data was considered as an instrument for the protection of privacy, and no distinction between the two rights was made. In *Scarlet*,[351] the Advocate General suggested that articles 7 and 8 of the Charter together, correspond to article 8 of the European Convention of Human Rights. In light of this reasoning, data protection would qualify as part of the right to a protected private life and not as an individual right, the same as discussed in a Council of Europe context. In *Promusicae*,[352] the CJEU identified a right to data protection but sees it as closely related to the right to a protected private life and refers to them as a single right. In *Schecke and Eifert*[353] the CJEU assimilates both articles 7 and 8 of the Charter to create a new right - the right to respect for private life with regard to the processing of personal data. This formulation might seem new in the framework of the CJEU's line of reasoning, but it is a reflection of the formulations that can be found in a number of EU legal acts as it is seen in the next section. In its decision the CJEU did not follow the opinion of the Advocate General Sharpstone[354] that distinguished between a classical right to privacy and a more modern right to protect the personal data. Data protection in this decision is seen as one of the aspects of the right to privacy of the individuals, information privacy. Privacy is therefore extended to include also the rules for the lawful processing of personal data. In *Schwarz*,[355] the CJEU considers processing of personal data to directly threat the right to privacy as well as the one to protection of personal data.

Important decisions showing the way the European Court has qualified the rights to privacy and data protection can be found in the *Bavarian Lager* case both from the General Court[356] in first instance and by the Court of Justice in the appeal case.[357] The case was about the request of Bavarian Lager to the European Commission to disclose the names of the participants at a meeting in which a decision against the company, in the field of competition law, was taken. The Commission did not disclose the names of 6 of the participants in the meeting which did not give their consent for such a disclosure. In first instance, the General Court found the decision of the Commission not to disclose the 6 names as unlawful. While clearly distinguishing between the right to privacy and the one to data protection, it found that the disclosure of names of the participants at a meeting was not a violation of their right to privacy. And while names would still be covered by the data protection rules, the General Court found that the exception of article 4(1)(b)[358] was applicable only in those cases in which the right to privacy of the individuals was infringed by the processing of personal data.[359] In this way, even if distinguishing the two rights, it suggested that legislation referring to data protection in the EU applies only when the right to privacy is involved.

[350] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 0031-0050
[351] Case C-70/10 Scarlet Extended [2011] ECR I-11959, Opinion of the AG Cruz Villalon, para. 31
[352] Case C-275/06 Promusicae [2008] ECR I-00271, paras. 64-65
[353] Case C-92/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, para. 52
[354] Case C-92/09 Volker und Markus Schecke and Eifert [2010] ECR I-11063, Opinion of AG Sharpstone, para. 71
[355] Case C-291/12 Schwarz v. Stadt Bochum EU:C:2013:670, paras. 29-30
[356] Case T-194/04 Bavarian Lager v. Commission [2007] ECR II-04523
[357] Case C-28/08P Commission v. Bavarian Lager [2010] ECR I-06055
[358] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, p. 43
[359] Case T-194/04 Bavarian Lager v. Commission [2007] ECR II-04523, para. 128

In the appeal case, the Court of Justice found that the General Court erred in law. While it is true that the right to privacy and the right to data protection are two distinguished rights, the CJEU found that the clause of article 4(1)(b)[360] is an indivisible provision requiring that any undermining of privacy and the integrity of the individual must always be assessed in conformity with the EU legislation on the protection of personal data, and does not allow to separate the processing of personal data into 2 categories (i.e. one examined in the light of the ECHR and Strasbourg case law, and the other subject to EU law).[361] As a result, personal data could not be separated into those examined in light of privacy and those examined for compliance with data protection rules.

The right to data protection was further clearly identified as an individual right by the CJEU in the *Deutsche Telecom* case.[362] In this case the CJEU stated that Directive 95/46 is designed to ensure in the Member States the right to protection of personal data. Also in its later decision on the invalidation of the *Data Retention Directive*[363] the CJEU draws a clear distinction between the two rights as contrasted to State interference for the purpose of prevention, investigation, detection and prosecution of serious crime. For the CJEU, what can be learned about the life of an individual on the basis of the electronic communications metadata retained on the bases of the Directive is quite extensive. This would include: habits of everyday life, permanent or temporary residences, daily or other movements, activities carried out, social relationships and social environments frequented and these interfere with the right to privacy.[364] The retention of personal data, however, involves also their processing. As a result there is simultaneously also an interference with the right to data protection.

From the above discussion of the case law from the European Courts it can be noticed that prior to the entry into force of the Lisbon Treaty, even if the Charter of Fundamental Rights existed as a non-binding document as of 2001, the CJEU considered the right to data protection as a subset of the right to privacy.[365] This is not surprising if one takes into account the way the right to data protection emerged and is qualified in the Council of Europe context. With the entry into force of the Charter as a binding legal instrument the treatment of the rights changed and now they are treated as two separate ones, even though in some situations the rights might still be confused. In the *Google* case, for example, the Advocate General[366] stated that "*the wide interpretation given by the Court to the fundamental right to private life in a data protection context seems to expose any human communication by electronic means to scrutiny by reference to this right*".

[360] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, p. 43
[361] Case C-28/08P Commission v. Bavarian Lager [2010] ECR I-06055, para. 59
[362] Case C-543/09 Deutsche Telecom [2011] ECR I-03441, para. 50
[363] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238
[364] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 27
[365] Lynskey, O. (2014) Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order, *International and Comparative Law Quarterly,* vol. 63, no. 3, pp. 569-597
[366] Case C-131/12 Google Spain and Google EU:C:2014:317, Opinion of the AG Costeja Gonzalez, para. 29

The confusion of the two rights has not remained confined only to the European Court of Justice decisions but it has been projected also in the doctrinal debate. Authors are divided into the ones that consider data protection as part of the right to privacy, and the ones that see these rights as differing from each other, even if they have very close links. The confusion between the two rights can be found also in documents from the European institutions. In a document on the challenges of science and research at global level, the European Commission stated that[367] the introduction of the right to data protection generates a technical conception of the right to privacy. In this light, privacy can be framed in terms of risk management, and technical ability to protect or to penetrate the private sphere with the use of personal data.

For De Busser (2009)[368] the aim of the right to privacy is different from the right to data protection. While the right to privacy is treated in her work as the respect for a person´s right to a personal development, the right to data protection, on the other side, is seen as protecting the data resulting from the interference with the right to privacy. In this line of reasoning a data protection assessment follows a privacy assessment. Only the methods of gathering data which are compatible with the derogations allowed to the right to privacy, and are therefore lawful in this light, will fall within the scope of application of the data protection legislation.[369] Also for Klitou (2014)[370] processing of personal data falls within the field of the right to privacy and Directive 95/46 is seen as providing guidance and establishing a set of criteria's for protecting this right.[371] For Brown and Korff (2009) the right to privacy is shorthand for a more specific right to "data protection" which apart protecting individuals from intrusions of their private life, protects them also from improper collecting, storing, sharing and use of their data.[372]

For other authors, the right to data protection is clearly related but not identical to the right to privacy.[373] For Gellert and Gutwirth (2013)[374] data protection is in certain aspects broader than privacy and in other aspects narrower. It is broader because it applies to processing of personal data even when they do not infringe upon privacy (as it is the case with publicly available personal information). In such situations, the privacy protection will not apply on processing of data that are not considered to affect one´s privacy. Data protection is considered by these authors at the same time also narrower than privacy because it only deals with the processing of personal data. Privacy

[367] European Commission (2012) Ethical and regulatory challenges to science and research policy at global level, Directorate General for research and innovation, p. 20
[368] De Busser, E. (2009) Data protection in EU and US criminal cooperation, Maklu Publishers, p. 52
[369] Idem, p. 66
[370] Klitou, D. (2014), Privacy invading technologies and privacy by design, Springer, p. 16
[371] Idem, p. 28
[372] Brown, I., Korff, D. (2009) Terrorism and the proportionality of internet surveillance, *European Journal of criminology*, vol. 6. No. 2, 119-134
[373] Hijmans, H., Scirocco, A. (2009) Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?, *Common Market Law Review*, vol. 46, Issue 5, pp. 1485–1525
[374] Gellert R., Gutwirth S. (2013) The legal construction of privacy and data protection, in *Computer Law & Security Review*, vol. 29, n. 5, pp. 522 - 530

might apply also to the processing of data that are not personal but that affect one's private life. An example of such data would be the details on the purchase of certain products online. The list of the products in itself does not constitute personal data since it cannot identify the individual person, but on the other side this list would give information on certain preferences of the purchaser and therefore interfere with his right to a protected private life.

For Kokott and Sobotta (2013)[375] the right to a protected private life differs from the right to data protection on a number of dimensions: the substantive scope, the personal scope and the obligations inferred. With regards to the substantive scope data protection is broader since it includes all information on identified or identifiable persons, even if this information is not private. With regards to the personal scope privacy is broader than data protection since it covers also the rights of legal persons.[376] With regards to the inferring of obligations data protection is broader than privacy since it puts obligations both on State authorities and on private parties.

For Gutwirth and De Hert (2006)[377] the difference between privacy and data protection is the one between opacity and transparency. Privacy is a tool of opacity that tends to guarantee non-interference in individual matters. Data protection is a tool of transparency that tends to guarantee the transparency and accountability of the controller of personal data. For these authors the right to privacy does prohibit certain arbitrary behaviours from the State while data protection does not prohibit behaviour but channels it into legitimate and normatively accepted powers. However, this division is not always as clear as above. Data protection can foresee for opacity rules (as in the case of sensitive data) while privacy can allow for transparency rules (as for example when telephone wiretapping is allowed).[378] In the same line argue Gutwirth and Hildebrandt (2010),[379] and add that the right to data protection is more specific than the right to privacy since it applies only when personal data are processed. For Korff (2014) data protection is a new *sui generis* right "*linked (but not limited to) the protection of privacy, or the interests of natural persons only*".[380]

[375] Kokott, J., Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law*, vol. 3, n. 4, pp. 222-228

[376] The authors base this on the case Bernh Larsen Holding AS and others v. Norway, ECHR application no. 24117/08, 14 March 2013, in this case however the Court refers to concerns for interference with the private life of all individuals working for the companies, and not to the rights of the companies themselves, paras. 104-107

[377] Gutwirth, S., De Hert, P. (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, pp. 61-104

[378] Gutwirth, S. (2007) Biometrics between opacity and transparency, *Annals of the Italian National Institute of Health,* vol. 43, no. 1, pp. 61-65

[379] Gutwirth, S., Hildebrandt, M. (2010) Some Caveats on Profiling, in S. Gutwirth, Y. Poullet & P. De Hert. (eds.), *Data protection in a profiled world*, Springer, pp. 31-41

[380] Korff, D. (2014) The rule of law on the internet and in the wider world, *Issue Paper published by the Council of Europe Commissioner for Human Rights*, available online at: https://wcd.coe.int/ViewDoc.jsp?id=2268589 (last accessed: 1.11.2014), p. 82

In other works as well as in a number of documents from the Article 29 Working Party,[381] the emergence of the right to data protection comes in a more declarative way, as the creation of the new right by the Charter. For Balducci Romano (2013)[382] the establishing of a level playing field in the processing of personal data serves the internal market as well as the individuals by giving them a new right which protects their dignity and personality, the right to data protection. For the Article 29 Working Party article 8 of the Charter regulates protection of personal data as a separate right, autonomous and different from the right to privacy[383] even though they are considered as closely linked.[384] For Rodota' the EU reinvented data protection by turning it into "*an essential tool to freely develop one´s personality*".[385] Data protection is seen as a proactive tool,[386] aiming to reduce the power of data controllers and processors as well as information asymmetries. The right to data protection provides individuals with more control over their personal data than the right to privacy would have been able to provide. For Cannataci (2008) a way to stop the debate about the nature of the rights would have been the introduction in the Charter of a pan-European principle of *ius personalitatis* including both the rights to privacy and data protection.[387]

3.4.2 Two separated rights

In the above discussions, despite the contradictions concerning the qualification of the rights to privacy and data protection as separate or as parts of the same right, it is commonly accepted that these rights are very closely linked to each other. Even if they are presented as two separated rights in the Charter of Fundamental Rights of the EU, the way the right to data protection historically evolved from the right to a protected private life, cannot be denied and influences its qualification. This author supports the line of reasoning that qualifies the two rights today as separate in the European Union context. This support is not built on any mechanical separation of the two rights that the EU legislator has done in the Charter but for the reasons that will be explained below.

[381] See Article 29 Directive 95/46/EC

[382] Balducci Romano, F. (2013) The Right to the Protection of Personal Data: A New Fundamental Right of the European Union, available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2330307 (last accessed: 11.2.2016), see also De Schutter, O. et al. (2006) The Commentary of the Charter of Fundamental Rights of the European Union, available online at: http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf (last accessed: 11.2.2016), p. 90; see also the editorial by Hustnix, P. (2013) The Increasing Horizontal Impact of Personal Data Protection, in *eucrim - The European Criminal Law Associations´ Forum,* no. 2013/1, pp. 1-2

[383] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007

[384] Article 29 Working Party, The future of privacy (2009) Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 1 December 2009, 02356/09/EN

[385] Rodota, S. (2009) Data protection as a fundamental right, in Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., Nouwt, S. (eds) *Reinventing Data Protection?*, pp. 77-82, Lynskey, O. (2014) Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order, *International and Comparative Law Quarterly,* vol. 63, no. 3, pp. 569-597

[386] Rodota, S. (2006) The European Constitutional Model for Data Protection, available online at: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/rodota_/rodota_en.pdf (last accessed: 11.2.2016)

[387] Cannataci, J. (2009) Lex personalitatis and technology-driven law, ScriptED, vol. 5, no. 1, pp. 1-6

Firstly, it is clear that the two rights have a different scope. While the right to privacy aims to protect the private life of the individuals from arbitrary interferences of State actors, the right to data protection focuses on the fair and legitimate collection and processing of personal data.[388] There is however an area where the two rights would meet and partially overlap with each other. This would be in those situations in which the collection and processing of the personal data interferes with the private life of the individuals – as it was the case with the invalidation of the Data Retention Directive. But while the right to privacy in such situations would focus on the aspects of the private life that have been interfered and the way this is performed, the right to data protection is concerned with the way the personal data is treated. In these cases, there is an overlap between information privacy (or data privacy) on the one side, and data protection on the other.[389] Data is a representation of information that can be stored, or transmitted and potentially manipulated. Information is the meaning that we give to data in a certain context.[390] The metadata from electronic communications are a clear example of such a situation. These data, once they are given a meaning, are able to give detailed information on the private life of an individual - with whom, how often and long one communicates. At the same time the way they are collected, processed and accessed has to comply with the data protection rules. There are of course other data that would fall only under the field of the right to privacy or only under the right to data protection.

Publicly available personal data, as for example the name of a person participating at a public meeting or a picture taken at a public place without identifying the person, would not fall under the protection of one's private life but is still treated under data protection rules (as it was reasoned in the *Friedl* case) since it qualifies as information relating to an identified or identifiable natural person.[391]

Collection of other personal data in a fair and legitimate way can be in conformity with the data protection rules (as for example the collection of fingerprints when applying for a passport), but still have an impact on the right to a protected private life of the individuals, and therefore the introduction of such rules must be checked with the privacy standards.[392] Other data that might give information on the life and preferences of a person might not qualify as personal data by themselves, as for example a list of products purchased online. However, because they are linked to an identified or identifiable person they need to comply both with the data protection as well as with the privacy rules.

[388] Mitsilegas, V. (2015) The transformation of privacy in the area of pre-emptive surveillance, Tilburg Law Review, vol. 20, pp. 35-57

[389] Some authors argue even that "information privacy" and "data protection" should be used as synonyms. See: De Hert, P., Papakostantinou, V. (2013) Three scenarios for international governance of data privacy: Towards an international data privacy organisation, preferably a UN agency?, *A Journal of Law and Policy for the Information Society*, vol. 9, no. 2, pp. 271-324

[390] Roosendaal, A. (2013) Protecting individuals' rights in online contexts, Wolf Legal Publishers, p. 10

[391] See definition of personal data in Article 2(a) of Directive 95/46/EC

[392] Case C-291/12 Schwarz v. Stadt Bochum EU:C:2013:670

Secondly, while the passive subject of both rights is a natural person,[393] there is a difference with regards to the active person of these rights. For the right to privacy the active person is the State and its actors. Article 8 ECHR explicitly protects individuals from arbitrary State interferences and, even if this is not explicit in article 7 of the Charter, this legal instrument is directed to the Union and its Member States.[394] The right to data protection can have as the active subject both the State and private actors, as for example in the field of the operation of Directive 95/46/EC that aims to protect individuals whose personal data are processed. If the right to data protection would have not emerged as a separate right from the one to privacy, then the secondary legislation at EU level would have been having a very limited effect for the protection of personal data in the hands of private actors. One can even argue that data protection has been used as the vehicle to protect information privacy not only in vertical relationships but also in horizontal ones that otherwise the right to privacy could alone not protect.[395] In this line of reasoning, the legislation has extended privacy by means of data protection rules and principles also in horizontal relationships and both rights incorporate elements from each other.

3.4.3 Concluding remarks

The aim of this section was to explore the protection of the right to privacy of individuals in the Charter of Fundamental Rights of the EU. It was presented that the Charter includes the right to a protected private life separating it from the right to data protection. The judicial and doctrinal debate justifying such a choice for separating the two rights at EU level was discussed. It was argued that the two rights are indeed separate and distinguished from each other but at the same time they are very close to each other with grey areas in which they overlap and make the distinction difficult.

When talking about interference with the private life of the individuals via surveillance with technologies not originally build for the purpose of surveillance, there can be different situations. One is of course to use the potential of the technology for direct surveillance. The other would be to make use of the data traces collected by the devices and programmes (dataveillance). What is relevant for this study is that the access to these data has a potential to interfere with the private life of the individual. The way the personal data are processed may fall under the data protection regime, under the protection of privacy (interfering with the "privacy of personal data" aspect of private life) or under both regimes simultaneously.

Thus, despite the separation of the rights, data protection rules might safeguard the right to privacy if an infringement of the right to data protection amounts at the same time to an infringement to the

[393] Contrary to this see: Kokott, J., Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law*, vol. 3, n. 4, pp. 222-228, these authors argue that the right to privacy covers applies also to legal persons

[394] Leczykiewitz, D. (2013) Horizontal application of the Charter of Fundamental Rights, *European Law Review*, vol. 38, pp. 479-497

[395] Case 101/01 Lindqvist [2003] ECR I-12971, para. 88

right to a protected private life.[396] That is the reason why in the following section both the EU legislation regulating the protection of the right to privacy as well as the right to data protection is scrutinized for assessing in how far they help to deal with the challenges created by surveillance with non-purpose built technology.

3.5 The primary and secondary EU law – Overlapping of the rights to privacy and data protection

This section is dedicated to the European Union primary and secondary legislation as well as to other EU legal acts that have as an aim to protect the rights to privacy and data protection of the European citizens. It has to be kept in mind that data protection has been used in the EU for protecting the right to privacy in those situations in which the two rights overlap. The section discusses also EU legislation that introduces measures that interfere with the rights to privacy and data protection of the individuals. This legislation is discussed for assessing the safeguards that they present for keeping these interferences into the limits of legality.[397]

In the aftermath of the tragic events of 11 September 2001, the EU became more aware of the role that it must play for securing the life and other fundamental rights of the EU citizens with a stronger focus on prevention of criminal acts and terrorist attacks. The impossibility of the use of existing data in European databases by law enforcement authorities was seen as a serious gap in the EU legislation of the time. The EU internal security strategy adopted in 2005, called thus for a proportionate and enhanced use of possibilities that already exist by interoperability, connectivity, synergy and availability of European databases.[398] Needless to say that such an approach creates more possibilities for surveillance with non-purpose collected data.

The same ideas were enforced the same year also in the form of the multiannual ´Hague Programme´ which called for a strengthening of the cooperation between law enforcement services of Member States for fighting terrorism and investigating cross-border crime effectively.[399] In this programme improved exchange of information as well as the creation of a European framework for protection of

[396] For example: collecting finger prints when applying for a visa would not violate the privacy of an individual if done in accordance with the rules, and the data collected have to be treated in conformity with the data protection principles. Accessing the fingerprint data against the data protection rules and process them to establish if the individual was present at a certain place in a given time, would infringe at the same time his right to privacy

[397] Loader, I. (2002) Policing, securitization and democratization in Europe, *Criminology and Criminal Justice*, vol. 2, no. 2, pp. 125-153

[398] COM(2005) 597 Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs

[399] COM(2005) 184 final, Communication from the Commission to the Council and the European Parliament of 10 May 2005 – The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice, OJ C 236, 24.9.2005

related data were suggested. The work of the Union towards a common model for criminal intelligence was set as a priority.

Information exchange with EU databases and within the Member States on a basis of mutual trust and based on the principle of information availability is discussed also in other non-binding legal acts.[400] A proactive approach based on prevention and anticipation and intelligence-led is suggested for the internal security of the European Union. In response to the Standard Eurobarometer 71[401] that concluded that four out of five Europeans want more action at EU level against organised crime and terrorism the new internal security strategy was adopted in 2010.[402] The need for more collaboration at EU level is related in this document with the international nature of criminal networks. More collaboration is requested from police, customs, border guards and judicial authorities in different Member States working alongside with European bodies, such as Europol and Eurojust. These elements are included also in the renewed internal security strategy for the years 2015-2020 which was presented by the Commission in April 2015.[403]

Together with the request for more collaboration and exchange of information between databases at EU level and Member States, also the protection of the fundamental rights of the individuals to privacy and data protection has been emphasized. The Stockholm Programme asked the Union institutions to respond to the challenges posed by the increasing exchange of personal data and to ensure the protection of the privacy of its citizens.[404] In that context the promotion of the application of the data protection principles as well as accession to Convention 108 is suggested.

In light of these security strategies and other documents of the European institutions a number of binding legal acts on collaboration and exchange of information at EU level and between the Member States have been adopted. This section will first elaborate on the EU primary law in the field. Than the secondary law is discussed focusing first on the general legislation on data protection and then on the one established for the creation of databases and exchange of information under the former first and third pillar. The Data protection reform package, including Regulation 679/2016 and Directive 680/2016, as well as its implications for surveillance with non-purpose built technology are presented at a separate section. The reform package was adopted after almost 4 years of discussions in April 2016 and will be enforced as of 2018.

[400] The European Council internal security strategy for the European Union - Towards a European Security Model, Brussels, 23 February 2010

[401] See Eurobarometer 71, available online at: http://ec.europa.eu/public_opinion/archives/eb/eb71/eb71_std_part1.pdf (last accessed: 22.11.2016), p. 148

[402] COM(2010) 673 final, Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Brussels, 22.11.2010

[403] COM(2015) 185 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security, Strasbourg, 28.4.2015

[404] The Stockholm Programme – an open and secure Europe serving and protecting citizens 2010/c 115/01

3.5.1 The primary EU law

With the entry into force of the Lisbon Treaty on the 1st of December 2009, articles regulating the right to data protection in the EU were introduced both at the Treaty of the European Union and the Treaty on the Functioning of the EU. The right to privacy is not explicitly regulated in the treaties.

Article 16 TFEU is important for introducing the right to data protection in the EU primary law although the founding principles of this right have already been incorporated in the Charter of Fundamental Rights. The Article is important also for introducing a legal base for adopting legislation on the basis of the ordinary legislative procedure in this field.[405] This gives the possibility to the Council and the Parliament to be both involved and co-decide the adoption of any proposals from the Commission in this field. The introduction of the legal base is important because in the absence it was difficult for the Union institutions to act in the field. This was especially seen in the case of the adoption of the Data Retention Directive.[406] In that case the Directive was adopted on the internal market legal basis so as to avoid the unanimity requirements of the flexibility clause in the first pillar or of the adoption of an intergovernmental act under the third pillar.[407] The old article 286 TEC on which article 16 TFEU is said to be based was only introducing the obligation on the EU institutions to comply with data protection rules. After the introduction of the Lisbon Treaty and the end of the pillar structure, article 16 TFEU should apply in all the areas of application of EU law. There is however an exception in the area of foreign and security policy which falls under the former second pillar of the EU.

In this area article 39 TEU gives the competence to the Council to adopt a decision laying down the rules relating to the protection of individuals with regards to the processing of personal data by the Member States. Article 39 TEU was introduced in Union law with the Lisbon Treaty. There was no specific provision on data protection in the area of Common Foreign and Security Policy beforehand. The article can be seen however as a procedural provision, establishing the way legal acts with the scope of protecting personal data will be adopted in the area of foreign and security policy. The substantive legal base on data protection remains the provision of article 16 TFEU. The article 39 TEU intergovernmental rule (giving power to the Council as an intergovernmental body to adopt decisions) will apply as an exception only for processing of personal data by the Member States and not by Union institutions and only in the area of foreign and defence policy. The decision by the Council in these situations needs unanimity voting for being adopted. This will enable national governments to keep the legislation in this area under their own control and it will allow individual Member States to veto any decision that they do not like. In this way, the Member States would prevent excessive interferences by Union policies with the activity of their national intelligence services.

[405] Article 294 TFEU

[406] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[407] Case C-301/06 Ireland v. Parliament and Council [2009] ECR I-00593

The derogation of article 39 TEU from article 16 TFEU has to be seen in a restrictive way.[408] This must be considered in light of the fact that according to article 275 TFEU, the Court of Justice of the EU does not have competence for viewing the legality of measures falling in the area of the common foreign and security policy nor with respect to acts adopted on the basis of those provisions. However, the Court of Justice does have jurisdiction to review the legality of any measures affecting individuals on account of Common Foreign and Security policies (article 275(2) TFEU). To the extent that such measures are adopted by the Council in the area of processing of personal data, the rules might become a matter on which the CJEU (albeit indirectly) might be called upon to decide. The way the second paragraph of article 275 TFEU will apply is left for clarification to future judicial decisions.

The elimination of the pillar structure and the introduction of the article 16 TFEU legal basis did not eliminate all the differences for the adoption of legal acts in the field of data protection for areas belonging to the former second and third pillar (Common Foreign and Security Policy and Police and Judicial Cooperation in Criminal matters).[409] With this regard the Lisbon Treaty contains two specific declarations of the intergovernmental conference which express the need for specific provisions in the area of judicial cooperation in criminal matters and police cooperation (Declaration no. 21), as well as in the area of national security (Declaration no. 20).

Declaration no. 21 states that "*specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on article 16 of the TFEU may prove necessary because of the specific nature of these fields*". Even though it is not completely clear what this Declaration implies in concrete terms, its wording suggests that for the former third pillar, specific rules may be evaluated as most appropriate, albeit using article 16 TFEU as the legal basis. The will of the Member States expressed in the Declaration was used as the justification for using article 16 TFEU as the legal basis for adopting Directive 2016/680 which is discussed in sub-section 3.6.2.[410]

Declaration no. 20[411] clearly provides for the need to take account of the "direct implications" that any data protection rules adopted under article 16 TFEU might have on national security taken in

[408] Blanke, J.-S., Mangiameli, S. (2013) The Treaty of the European Union - A commentary, Springer, p. 1167

[409] See Scirocco, A. (2008) The Lisbon Treaty and the protection of personal data in the European Union, *Data Protection Review*, no. 5, available online at: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2008/08-09-19_Scirocco_Lisbontreaty_DP_EN.pdf (last accessed: 11.2.2016)

[410] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[411] Declaration no. 20 on the application of Article 16 TFEU states: "*The Conference declares that, whenever rules on protection of personal data to be adopted on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. It recalls that*

consideration the specific characteristics of the subject. By referring to the limitation of the scope of Directive 95/46/EC[412] the same limitations are declared to apply also for the use of article 16 TFEU in the area of national security. In this context, it should be highlighted that, even if declarations are not binding legal instruments they have a strong political value since they express the will of the Member States when adopting the binding provisions and will guide the interpretation and application of the relevant provisions, though this must not jeopardize the protection of fundamental rights in the field.[413]

3.5.2 The secondary EU law

After the primary legislation, due attention must be paid also to the secondary legislation at European Union level. The focus of this sub-section is not just on the legislation protecting the right to privacy and data protection (since, as already seen, not respecting data protection rules might have implications for privacy as well). But the focus is also on those provisions that would qualify as measures of surveillance because they regulate interference from the State with the private life of the individuals. Most of the secondary legislation in this field predates the entry into force of the Treaty of Lisbon, therefore reflects the pillar structure of the EU as well as the not yet official separation between the rights to privacy and data protection. One has to keep in mind, however, that the Charter of Fundamental Rights of the EU was adopted in the year 2000 - therefore the identification of the right to data protection as individual right and separated from the right to privacy dates back at that time. The aim of this sub-section is not only to identify the relevant legal acts but also to assess in how far the secondary EU legislation protects the right to privacy of the individuals from State interferences and if there are insights that might be used for addressing the challenges created by surveillance with non-purpose built technology. The new data protection reform package is discussed in the following section.

a) Data protection Directive

The most important secondary legal instrument is Directive 95/46/EC on processing personal data and their free movement.[414] The processing of personal data in this Directive is seen as part of the right to privacy and already in article 1(1) it is stated that the object of the Directive is for the Member States to protect fundamental rights and freedoms of natural persons, "*and in particular their right to privacy with respect to the processing of personal data*."

---

the legislation presently applicable (see in particular Directive 95/46/EC) includes specific derogations in this regard."

[412] See article 3(2) of Directive 95/46/EC

[413] Article 67 TFEU

[414] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995, pp. 0031 – 0050; Poullet, Y. (2006) EU data protection policy. The Directive 95/46/EC: Ten years after, in *Computer Law and Security Review*, vol. 22, no. 3, pp. 206-217

So, processing of personal data is seen as having a special relation with privacy interferences. Data protection has been used in this Directive as the vehicle to protect privacy, not only in vertical relationships but also in horizontal ones that otherwise the right to privacy could alone not protect.[415] The Directive explicitly excludes from its scope of application activities that fall in the areas of public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.[416]

The Directive is adopted as an internal market instrument, though in *Rundfunk*[417] the CJEU highlighted that if an effective connection to the internal market had to be checked in each case, the scope of application of the Directive would be particularly unsure and uncertain. Regarding its scope of application, in the *PNR* judgement the CJEU considered that article 3(2) of the Directive applies also when the transfer of data falls within the framework established by public authorities that relates to public security.[418] It does not only cover public authorities but also private parties that are obliged to support their activities. Such a statement in the judgement leaves the effective protection of the individuals unregulated in those situations in which commercial data are further processed for law enforcement purposes.[419]

Articles 6 and 7 of this Directive are especially important in as much as they express the principles for processing personal data (article 6) and the criteria for legitimating this process (article 7). According to article 6 the processing of personal data must be:

(a) fair and lawful;

(b) the data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and kept up to date;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

[415] See the definitions of "controller" and "processor" of personal data in Article 2(d) and (e) of the Directive 95/46/EC; Case 101/01 Lindqvist [2003] ECR I-12971, para. 88
[416] See article 3(2) of Directive 95/46/EC
[417] Joined Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others [2003] ECR I-04989, para. 41
[418] Joined Cases C-317 & 318/04, European Parliament v. Council and Commission, [2006]ECR I-4721, para 58
[419] Hijmans, H., Scirocco, A. (2009) Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?, in *CMLR*, vol. 46, no. 5, pp. 1485-1525

According to article 7 personal data must be processed only in a number of well identified situations: (i) if the data subject has unambiguously given his consent, or (ii) processing is necessary for the performance of a contract to which the data subject is party, or (iii) processing is necessary for compliance with a legal obligation to which the controller is subject, or (iv) processing is necessary in order to protect the vital interests of the data subject, or (v) processing is necessary for the performance of a task carried out in the public interest, or (vi) in the exercise of official authority vested in the controller, or (vii) in a third party to whom the data are disclosed, or (viii) processing is necessary for the purposes of the legitimate interests pursued by the controller, or by the third party, or parties to whom the data are disclosed.

The Directive creates also the Article 29 Working Party composed of representatives from the data protection authorities of each Member State, the European Data Protection Supervisor and the European Commission. The Working Party does not have any executive powers and its tasks are to:

- give expert advice to the Member States regarding data protection;
- promote the same application of the Directive in all the Member States;
- give its opinion to the Commission on Union laws affecting the right to protection of personal data.

However, even if it establishes principles on the collection and processing of personal data both by State authorities and by service providers, the reach of this Directive in the area of state surveillance is limited. As said above, the Directive does not apply in the areas of public security, defence, State security and the activities of the State in areas of criminal law. As a result, also State surveillance in general, with purpose built or non-purpose built technology, will not fall in the field of application of the Directive. As of the 25th of May 2018, this Directive will not exist anymore due to the new Regulation 2016/679 (discussed in the following section) that repeals it.

b) Electronic communication Directive

While the Data Protection Directive is designed as a framework one and applies any time personal data are processed, other legislation at EU level is more specific. Directive 2002/58/EC[420] operates in the field of electronic communications and the processing of personal data in this field. The aim of the Directive is to protect the right to privacy which might be infringed in those situations in which the principles for the processing of personal data are infringed.[421]

[420] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002, pp. 0037 - 0047

[421] See Art. 1(1) of Directive 2002/58/EC

The Directive is adopted as an internal market instrument and its aim is to ensure the confidentiality of the communications and other metadata by prohibiting any listening, tapping, storage or other kinds of interception or surveillance of communications when the consent from the data subject is missing or no legal authorization is given.[422] Traffic data must also be erased or made anonymous when it is no longer needed for the purpose of transmission of a communication.[423] Location data is allowed to be processed but only when made anonymous.[424]

The provisions of this Directive are not intended to cover activities of the State which fall in the area of public security, defence, State security and the activities of the State in the area of criminal law.[425] They are directed to service providers. As a result, the Directive would not cover surveillance activities by the State. For extending the activities of service providers and their collaboration with the State the Directive requires the introduction of legislation at national level to restrict exceptionally the rights and obligations provided for in the Directive in those situations in which the interference will constitute a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences, etc.[426] In the amendment that was done to article 4 of this Directive,[427] one can see that the legislator is trying to distinguish between an interference with the personal data and an interference with the privacy of the subscriber, even if this distinction is not further elaborated in the legal document.[428] At the time of writing, the Commission has initiated the procedures for adopting a new Regulation on electronic communications which has to be in line with the reformed data protection package and will repeal the Directive.[429]

c) Regulation on data processing by EU institutions

Also Regulation 45/2001/EC[430] is adopted as an internal market instrument based on article 286 EC. It deals with the protection of individuals' right to privacy that might be infringed when personal data

[422] See article 5(1) of Directive 2002/58/EC
[423] See article 6(1) of Directive 2002/58/EC
[424] See article 9(1) of Directive 2002/58/EC
[425] See article 1(3) of Directive 2002/58/EC
[426] See article 15(1) of Directive 2002/58/EC
[427] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), OJ L 337, 18.12.2009, pp. 11–36
[428] See the provision amending article 4 of Directive 2002/58/EC that reads: "*When the personal data breach is likely to adversely affect the personal data or privacy of the subscriber or individual, the provider shall also notify the subscriber or individual of the breach without delay*."
[429] COM(2017) 10 final Proposal for a Regulation of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC
[430] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, pp. 1–22

are processed by Union institutions. The lawfulness of processing personal data is linked for this Regulation with the performance of tasks carried out in the public interest; with the necessity to comply with the legal obligations of the controller, with the performance of a contract in which the data subject is a party, with the unambiguous consent or with the protection of vital interests of the data subject.[431]

The Regulation creates the European Data Protection Supervisor whose task is to monitor the application of the provisions of this legislation to all data processing operations carried out by EU institutions or other bodies.[432] The Regulation introduces also the concept of prior checking for all processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature or their scope. This prior checking task is performed by the European Data Protection Supervisor.[433]

d) Regulation on biometric passports

Another relevant law adopted on the bases of the former first pillar is Council Regulation 2252/2004[434] on the introduction of biometric data in the passports of EU citizens. These data consist in facial image and fingerprints with the aim to harmonise national legislation and to make fight against fraud and falsification of the documents more effective.[435] The regulation does not create a centralized storage for the collected data which are stored in the document itself and exclusively for the purpose of issuing passports and travel documents.[436] The biometric features in passports and travel documents cannot be used for other purposes than the verification of the document and the identity of the holder. Thus, the Regulation does not give cause to surveillance with non-purpose collected data. This legislative choice, together with the fact that no centralized data storage is provided, were saving the regulation from a possible annulment for non-compliance with the principle of proportionality.[437]

3.5.3 EU legislation for creation of databases and exchange of information – former first pillar

In this sub-section, a number of legal acts adopted in the EU for the creation of databases and exchange of information between the Member States are discussed. It has to be kept in mind that collection and processing of information does not qualify only under data protection rules. The European Court of Justice ruled that systematic retention of personal data qualifies as surveillance of

[431] See article 5 Regulation (EC) No 45/2001
[432] See article 1(2) Regulation (EC) No 45/2001
[433] See article 27 Regulation (EC) No 45/2001
[434] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385/1, 29.12.2004
[435] See article 1(2) Council Regulation (EC) No 2252/2004
[436] See article 4(3) Council Regulation (EC) No 2252/2004
[437] Case C-291/12 Schwarz v. Stadt Bochum EU:C:2013:670, para. 61

the citizens.[438] That is why laws introduced for the retention of personal data apart complying with the data protection rules, must comply as well with the privacy safeguards.

a) EURODAC

Regulation 2725/2000/EC introduced at European level EURODAC.[439] This is a database for the collection, storage, transmission and comparison of fingerprints for applicants for asylum, aliens and recognized refugees. EURODAC consists of a central system which operates a computerized central database of fingerprint data, as well as of the electronic means of transmission between the Member States and the Central System. It also establishes rules on the data use, data protection and liability as well as rights of the data subject. This Regulation did not provide for access to the database from law enforcement authorities but its validity expired on the 20th of July 2015. As of that date, Regulation no. 603/2013/EU,[440] adopted in light of the Hague Programme, become applicable. Apart regulating the way fingerprints are being collected and stored as in the previous Regulation, the new Regulation opened the possibility to national law enforcement authorities as well as to Europol to access the collected fingerprints data for comparisons for the scope of prevention, detection, or investigation of terrorist offences and of other serious crimes.[441]

The possibility to access the data is considered as a necessity for the prevention, detection or investigation of terrorist offences,[442] however such access is a change of the original purpose of data collection and as such qualifies as surveillance with non-purpose collected data. It has to be kept in mind that the fingerprints data of all applicants for asylum, aliens and recognized refugees are stored in the data base. As a result, even if in compliance with the law and data protection rules, the access to the personal data interferes with the right to a protected private life of the data subjects. That is the reason why access to the data is required to be in conformity with the legal principles of necessity and proportionality.[443] For respecting the rights to data protection and excluding systematic comparison of the personal data, access should take place only in specific cases, when there is a specific situation[444] and an overriding security concern.[445]

[438] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 37
[439] Council Regulation (EC) no 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15/12/2000
[440] Regulation (EU) no 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)
[441] See article 5-7 Regulation (EU) no 603/2013
[442] See recital 8 Regulation (EU) no 603/2013
[443] See recital 13 Regulation (EU) no 603/2013
[444] See recital 31 Regulation (EU) no 603/2013
[445] See recital 10 and article 21 Regulation (EU) no 603/2013

b) VIS

Regulation 767/2008/EC[446] deals with the creation of a common Visa Information System (VIS) and the exchange of data between Member States on short-stay visas. This Regulation provides the conditions and procedures for the exchange of personal data between the EU Member States and associated countries applying the common visa policy. Thus, the aim of the Regulation is that examination of applications for short stay visas and decisions on extending, revoking and annulling visas, as well as the checks on visas and the verifications and identifications of visa applicants and holders are facilitated. Personal data from all the applicants for short-stay visas are stored in the database. The VIS Regulation provides for the access in the database from designated State authorities and Europol if there are reasonable grounds to consider that VIS data will substantially contribute to the prevention, detection or investigation of terrorist offences and of other serious crime offences. Thus, surveillance with non-purpose collected data is allowed even though only in specific cases and after a reasoned request.[447]

c) SIS II

On 9 April 2013, the second generation Schengen Information System (SIS II) as a large-scale information system containing alerts on persons and objects entered into operation.[448] By allowing for easy information exchanges between national border control, customs and police authorities, it ensures that the free movement of people within the EU can take place in a safe environment. SIS II has enhanced functionalities, such as the possibility to use biometrics, new types of alerts, the possibility to link different alerts (such as an alert on a person and a vehicle) and a facility for direct queries on the system. Access to this data is allowed for border security authorities as well as for national judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to the charge in accordance with national legislation.[449]

d) eu-LISA

For the management of EURODAC, the Visa Information System (VIS) and the second-generation Schengen Information System (SIS II) a European agency (eu-LISA) in the form of an independent body with legal personality is created.[450] The main task of eu-LISA is to keep the systems under its responsibility functional to ensure the continuous and uninterrupted exchange of data between

[446] Regulation (EC) no 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, pp. 60-81

[447] Article 3(1) Regulation (EC) no 767/2008

[448] Regulation (EC) no 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006, pp. 4–23

[449] See article 27 Regulation (EC) no 1987/2006

[450] Regulation (EU) no 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011, pp. 1–17

national authorities.[451] The agency is also responsible for adopting and implementing security measures, organising training for IT experts on the systems under its management, reporting, publishing statistics and monitoring research activities. The agency has to ensure that security and data protection requirements are fully met in the systems it manages.[452]

e) The passenger name record (PNR) directive

In May 2016, a Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime was adopted.[453] The adoption followed a request by the European Council of the 25 and 26 of March 2004, in the aftermath of the terrorist attacks in Madrid.

PNR data are stored in the carriers' reservation systems. They include the name, travel dates, travel itinerary, ticket information, contact details, travel agent at which the flight was booked, means of payment used, seat number and baggage information. These data have already been used by Member States' law enforcement bodies in specific cases either on the basis of specific legislation or on the basis of general legal powers. The Directive harmonizes the approach to PNR data across the EU. It establishes that the data collected may only be processed for the purpose of prevention, detection, investigation and prosecution of terrorist offences and serious crime. The scope of application of the Directive distinguishes it from the existing Council Directive 2004/82[454] on the basis of which data retained by carriers are transferred to the competent national authorities only for the purpose of improving border controls and combating illegal immigration.

Under the provisions of the Directive, air carriers will be obliged to provide Member States' authorities with the PNR data for flights entering or departing from the EU. It will also allow, but not oblige, Member States to collect PNR data concerning selected intra-EU flights.[455] The Directive, which will be enforced as of the 25th of May 2018, creates an EU standard for the use of PNR data. Its provisions regulate the purposes for which PNR data can be processed, exchanged and stored. It incorporates safeguards as regards protection of privacy and personal data, including the role of national supervisory authorities and the mandatory appointment of a data protection officer in the Passenger Information Units created in the Member States. It also includes the concept of depersonalization of data through masking out the elements which could serve to identify directly the passenger to whom the data relate.[456]

[451] See articles 3-7 Regulation (EU) no 1077/2011
[452] See article 2(e) and (f) Regulation (EU) no 1077/2011
[453] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016, pp. 132–149
[454] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, pp. 24-27
[455] Article 2, PNR Directive
[456] Article 12(2) PNR Directive

3.5.4 Collaboration between the Member States – former third pillar

In this sub-section are explored a number of legal acts adopted in the area of justice and home affairs and aiming at the collaboration and exchange of information between the Member States. It has to be kept in mind that before the entry into force of the Treaty of Lisbon this area belonged to the third pillar of the European Union and allowed only for the adoption of intergovernmental decisions. The competence of the Union in this area was limited.

a) Framework decision on police and judicial cooperation

The most important piece of legislation in this field is the Framework Decision 2008/977/JHA[457] on the protection of personal data in the framework of police and judicial cooperation in criminal matters. The adoption of this act after the adoption of the EU Charter of Fundamental Rights is reflected in the preamble where the right to data protection and the one to privacy are considered as two separate rights.[458] In the text of the act, however, the same formulation as in other legal documents is found: "…*protecting the right to privacy, with respect to the processing of personal data*…".[459] The provisions of the decision apply only when Member States are transmitting data between them. The processing of data within the Member States for the purpose of internal needs in the area of law enforcement does not fall within the scope of application of this framework decision and is left for regulation by national rules.

The principle of purpose limitation for the collection of personal data occupies a central role in this decision. It is stated that personal data may be collected only for specified, explicit and legitimate purposes and may be processed only for the same legitimate purpose for which they were collected.[460] Further processing of the data for another purpose are permitted exceptionally and in so far as they: (i) are not incompatible with the purpose for which the data were collected; (ii) there is an authorization in compliance with the applicable legal provisions; (iii) and processing is necessary and proportionate to the other purpose.

While the above Framework decision is general, also more specific acts for collaboration between the Member States have been adopted. In cases of interception of telecommunications between countries, for example, the Convention on mutual assistance in criminal matters establishes that the State of the interception is required to collaborate with the intercepting country, and possibly to make it directly accessible for the lawful interception by that Member State through the

[457] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, pp. 60-71
[458] See recital 3 and recital 48 Council Framework Decision 2008/977/JHA
[459] See article 1(1) Council Framework Decision 2008/977/JHA
[460] See article 3(1) Council Framework Decision 2008/977/JHA

intermediary of a designated service provider present in its territory.[461] If no technical assistance is needed to carry out the interception, the intercepting Member State shall inform the Member State in which territory the interception is taking place about the interception.[462] This Framework decision will apply only till the 6th of May 2018. After that date, Directive 2016/680 becomes applicable.

b) European Evidence Warrant

The collaboration between the Member States is extended also with regards to the Framework Decision 2008/978/JHA on the European Evidence Warrant (EEW).[463] This warrant has the purpose to exchange between the Member States objects, documents and data for use in proceedings in criminal matters. The EEW cannot be used for asking the collection of new personal data,[464] but it can be used for asking the transfer of personal data that are already in the database.[465] This exchange of data is done in light of the principle of availability.

The collaboration of the Member States in the EEW was seen as positive and some Member States took the initiative to bring their collaboration further with the proposal of a Directive on the European Investigation Order (EIO) in criminal matters.[466] One of the main changes of the EIO compared to the EEW is that the EIO is based on an investigative measure to be executed while the EEW is based on a specific type of evidence to be obtained. EIO also covers administrative proceedings having a criminal dimension. EIO is a judicial decision which has been issued or validated by a judicial authority of a Member State to have one or several specific investigative measure(s) carried out in another Member State to obtain evidence. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State.[467]

c) Framework decision on exchange of information and intelligence

Exchange of information and intelligence between the Member States is the aim also of the Council Framework Decision 2006/960/JHA.[468] The Decision establishes the rules under which Member

[461] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, pp. 1-23, article 19

[462] Convention on mutual assistance in criminal matters, article 20

[463] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L 350, pp. 72-92

[464] Article 4(2) Council Framework Decision 2008/978/JHA

[465] Article 4(4) Council Framework Decision 2008/978/JHA

[466] See initiative by Belgium, Bulgaria, Estonia, Spain, Austria, Slovenia and Sweden, available online at: http://ec.europa.eu/justice/news/intro/doc/comment_2010_08_24_en.pdf

[467] See article 1(1) of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1–36

[468] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89–100

State's law enforcement authorities may exchange existing information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations.[469]

The Decision defines criminal investigation as a procedural stage within which measures are taken by competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several identified concrete criminal acts.[470] Criminal intelligence operation on the other side is defined as a procedural stage, not yet having reached the stage of criminal investigation, within which a competent law enforcement authority is entitled by national law to collect, process and analyse information about crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future.[471]

Information and intelligence may be requested for the purpose of detection, prevention or investigation of an offence where there are factual reasons to believe that relevant information and intelligence is available in another Member State. The request shall set out those factual reasons and explain the purpose for which the information and intelligence is sought and the connection between the purpose and the person who is the subject of the information intelligence.[472] The use of information and intelligence which has been exchanged directly or bilaterally under this framework decision shall be subject to the national data protection provisions of the receiving Member State, where the information and intelligence shall be subject to the same data protection rules as if they had been gathered in the receiving Member State.[473]

d) Framework decision on the exchange of information extracted from criminal records

Council Framework Decision 2009/315/JHA[474] on the organisation and content of the exchange of information extracted from the criminal record between Member States aims to complement the existing general rules on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters in the EU.

The objectives of this Framework decision are to:[475]

[469] Article 1.1 Council Framework Decision 2006/960/JHA
[470] Article 2(b) Council Framework Decision 2006/960/JHA
[471] Article 2(c) Council Framework Decision 2006/960/JHA
[472] Article 5(1) Council Framework Decision 2006/960/JHA
[473] Article 8(2) Council Framework Decision 2006/960/JHA
[474] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93, 7.4.2009, pp. 23–32
[475] Article 1 Council Framework Decision 2009/315/JHA

- define how a convicting Member State is to transmit information on the conviction to the Member State of which the convicted person is a national;
- define the obligations of the Member State of which the person is a national to store information on convictions and the procedures which that Member State is to follow when replying to requests for information about its nationals;
- establish a framework for the development of a computerised system of exchange of information on convictions.

Member States are to designate a central authority to carry out the tasks relating to exchanges of information on convictions. For transmitting information and for replying to a request for information, Member States may designate more than one central authority.[476]

e) Council decision on the exchange of information extracted from criminal records

Council Decision 2005/876/JHA[477] on the exchange of information extracted from the criminal record establishes limits for the receiving Member States which must use personal data communicated for the purpose of criminal proceedings only for the purpose of the criminal proceedings for which it has been requested.[478] Personal data communicated for purposes other than criminal proceedings, may be used by the requesting Member State in accordance with its national law only for the purpose for which it has been requested and within the limits specified by the requested Member State in the form.[479]

f) Framework decision for exchange of information between authorities responsible for prevention and investigation of criminal offences

The purpose of Framework Decision 2008/615/JHA is to step up cross-border police and judicial cooperation between Member States in criminal matters.[480] Especially it aims to improve the exchanges of information between the authorities responsible for the prevention and investigation of criminal offences.

The Decision includes provisions on:[481]

[476] Article 3(1) Council Framework Decision 2009/315/JHA
[477] Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record, OJ L 322, 9.12.2005, pp. 33-37
[478] Article 4(1) Council Decision 2005/876/JHA
[479] Article 4(2) Council Decision 2005/876/JHA
[480] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008, pp. 1-11
[481] Article 1 Council Decision 2008/615/JHA

- the conditions and procedure for the automated transfer of DNA profiles, dactyloscopic data and certain national vehicle registration data (Chapter 2);
- the conditions for the supply of data in connection with major events with a cross-border dimension (Chapter 3);
- the conditions for the supply of information in order to prevent terrorist offences (Chapter 4);
- the conditions and procedure for stepping up cross-border police cooperation through various measures (Chapter 5).

Detailed rules are directed to Member States for guaranteeing that personal data processed according to this decision is protected by their national laws. Only the relevant competent authorities may process personal data. They must ensure the accuracy and current relevance of the data. Steps must be taken to rectify or delete incorrect data or data that was supplied when it should not have been. Personal data must be deleted if no longer needed for the purpose it was made available or if the storage time, as provided by national law, has expired.[482]

In order to maintain oversight and coordinate the cooperation between the Member States in the area of justice and home affairs also a number of bodies are created to operate at EU level. Below Eurojust and Europol will be discussed in turn.

g) Eurojust

To step up cooperation in the fight against crime, the Tampere European Council decided to set up a unit called Eurojust,[483] with the objective of coordinating the activities carried out by national authorities responsible for prosecution and supporting criminal investigations in organised crime cases. Following this, Decision 2002/187/JHA establishes Eurojust as a body of the Union with legal personality and a judicial coordination unit.[484] With the entry into force of the Treaty of Lisbon, Eurojust is incorporated also in article 85 TFEU where its mission is defined: "*to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States…*".

[482] Articles 24-32 Council Decision 2008/615/JHA

[483] See Tampere European Council Conclusions, available online at: http://www.europarl.europa.eu/summits/tam_en.htm (last accessed: 29.4.2015), para. 46

[484] Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 063, 6.3.2002, pp. 0001-0013, amended by Council Decision 2003/659/JHA of 18 June 2003 and Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust

Each Member State must appoint a national member to Eurojust headquarters: a prosecutor, judge or police officer (the latter must have competences equivalent to the judge's or the prosecutor's).[485] Eurojust's competence covers, *inter alia*, the types of crime and offences for which Europol has competence such as terrorism, drug trafficking, trafficking in human beings, counterfeiting, money laundering, computer crime, crime against property or public goods including fraud and corruption, criminal offences affecting the European Union's financial interests, environmental crime and participation in a criminal organisation. For other types of offences, Eurojust may assist in investigations and prosecutions at the request of a Member State.[486]

In order to realise its objectives, Eurojust must be able to exchange data with the competent authorities. To this end, the application of the principles of the Council of Europe Convention 108 must be guaranteed.[487]

Eurojust may only process data on persons who are either suspected of having committed, or have been convicted of an offence for which Eurojust has competence or are victims and witnesses to such crimes. The types of data that can be used include the person's identity (full name, date and place of birth, nationality, contact details, profession, social security numbers, identification documents, DNA profiles, photographs, fingerprints, etc.) and the nature of the alleged offences (criminal category, date and place of the offence, type of investigation, etc.).[488]

h) Europol

The European Police Office known as Europol is established with legal personality. Its aim, as the European Union's enforcement agency is to improve the effectiveness of, and cooperation between, the competent authorities in Member States in preventing and combating international organised crime.[489] Unlike the police services of Member States, Europol does not have executive powers. It cannot detain individuals, nor can it conduct home searches. Its tasks are to facilitate the exchanges of information, analyse intelligence and coordinate operations involving several Member States. Europol offices comprise both law enforcement and intelligence powers blurring in this way the borders between the two.[490]

[485] Article 2 Council Decision 2002/187/JHA
[486] Article 4 Council Decision 2002/187/JHA
[487] Article 14 Council Decision 2002/187/JHA
[488] Articles 14-15 Council Decision 2002/187/JHA
[489] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016, pp. 53–114
[490] Deflem, M. (2006) Europol and the policing of international terrorism: Counter-terrorism in a global perspective, *Justice Quarterly*, vol. 23, no. 3, pp. 336-359; Svedsen, A.D.M. (2011) On 'a Continuum with expansion'? Intelligence co-operation in Europe in the early twenty-first century, *Journal of Contemporary*

To perform its tasks, Europol maintains an IT database. Under no circumstances may this database be linked to other automated processing systems, except for the systems of the national units. The national units are responsible for the security of data-processing equipment and for carrying out checks on the storage and deletion of data files. The system is made up of three components: the IT information system, work files and index system.[491]

The information system may only be used to store, modify and utilise data that are necessary for the performance of Europol's tasks. The system does not contain data on related criminal offences. The data concern persons who, under the national law of a Member State, are suspected of having committed or having taken part in a criminal offence for which Europol is competent or who have been convicted of such an offence. The system also contains data concerning persons who are suspected of planning to commit criminal offences for which Europol is competent.[492]

Member States ensure a standard of data protection under their national legislation that must at least correspond to the Council of Europe Convention 108 and of Recommendation No R (87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987.[493] Each Member State must ensure that the data it transmits to Europol are legal, accurate and up to date, and check the storage time limits. Europol is responsible for data transmitted to it by third parties or resulting from analyses that it has carried out. As of the 1st of May 2017, the supervision of the data protection regime for Europol will be carried out by the EDPS.[494]

3.5.5 Concluding remarks

The aim of this section was to identify the primary and secondary EU legislation for the protection of the rights to privacy and data protection of EU citizens and to assess in how far insights from these laws could be used in cases of surveillance with non-purpose built technology. It was found that the EU legislation is mainly focusing on data protection and due to the historical separation of the competences of the EU in three different pillars its reach for activities of law enforcement authorities is still limited. The protection offered is technology neutral.

Even though there are no specific laws on surveillance, traditional or with non-purpose built technology, the creation of a number of data bases giving access to law enforcement authorities for

European Research, vol. 7, no. 4, pp. 520-538; Zavesnik, A. (2013) Blurring the line between law enforcement and intelligence: Shaping the gaze of surveillance?, *Journal of Contemporary European Research*, vol. 9, no. 1, pp. 181-202

[491] Article 11 Council Decision 2009/371/JHA

[492] Article 12 Council Decision 2009/371/JHA

[493] Article 27 Council Decision 2009/371/JHA

[494] Article 43 Regulation 2016/794

the purpose of prevention, detection, investigation and punishment of crime has to be noted. In these databases are collected and stored personal data of citizens that apply for benefiting from specific rights but on the bases of the principle of availability of information the data might be further used by law enforcement authorities. It thus creates situations of dataveillance, of surveillance with non-purpose collected data and potential use for mass surveillance and retroactive surveillance.

For safeguarding the rights of the individuals, the access to these databases is limited to specific cases and in conformity with the principles of necessity and proportionality. The latter, aim to insure the protection of the right to privacy also in those situations in which the right to data protection is safeguarded. The legislation also aims to ensure the training of IT experts in charge of the databases created at EU level for ensuring that security and data protection requirements are fully met. For ensuring the security of the data, the new PNR Directive introduced the concept of depersonalization of the data after 6 months that they are transferred to the passenger information unit. The following of these safeguards would help also for bringing surveillance with non-purpose built technology into the realm of lawfulness.

The strengthening of the cooperation between the Member States for the exchange of information on the basis of the principles of mutual trust and information availability does not follow for harmonization of the national rules on obtaining evidence. Thus, different national standards are used for the later.

The entry into force of the Treaty of Lisbon introduced a single legal basis for the adoption of legislation in the area of data protection in article 16 TFEU. The article has however its limitations since: (i) it focuses only on data protection and not on the protection of the right to privacy in general; (ii) has limitations in the area of foreign and defence policy (were the more stringent requirements of article 39 TEU are to be followed). In the following section is discussed the new Data Protection reform package that will become applicable as of May 2018.

3.6 The new Data Protection package – Harmonisation of national law enforcement activities

The quick development of technology accompanied with the large scale exposure, collection and use of personal data needs to be matched by adequate rules for the protection of the rights of the individuals. The dimensions of the technology driven society in which we live today were not predicted in 1995 when the Data Protection Directive was adopted and make it difficult for its provisions to cope with reality. The 2008 Framework Decision on Police cooperation, even though more recent, focuses only on the exchange of data between the Member States and not on the standards on the protection of personal data by law enforcement. The proposal from the

Commission in January 2012 for the adoption of a new data protection package has, thus, been long awaited and welcomed.

In the era in which we live, the new data protection package has to fulfil a double objective. On one side, it must give back to the citizens the control over their personal data and, on the other side, it must simplify the regulatory environment for businesses. The data protection reform is seen as a key enabler of the Digital Single Market which the Commission has prioritized in its work.

The reform package as such aims to:[495]

i. Create a single set of comprehensible rules in the field;
ii. Strengthen the rights of the data subjects;
iii. Increase the responsibility and the accountability of controllers and processors of data;
iv. Remove the unnecessary administrative burdens for the business;
v. Strengthen the enforcement framework.

The potential effect that the data protection reform package will have for the business environment and the lobbying process that was linked to it were definitely the ones that slowed down its adoption. After a lengthy legislative process and many months of negotiations, the reform package was finally adopted in April 2016. It consists of two legal instruments, a regulation and a directive. The General Data Protection Regulation regulates the field that is thus far covered by the 1995 Data Protection Directive. The new Data Protection Directive regulates the protection of personal data when used by law enforcement for the scope of prevention, detection, investigation and prosecution of crime and repeals the 2008 Framework Decision.

Article 16 TFEU was used as the legal basis for the adoption of both legal instruments. Even if the Article itself does not seem to cover the field of judicial cooperation in criminal matters and police cooperation, the Member States declared[496] their consent for the use of this article as a legal basis for the adoption of legislation in the field.[497] Both legal instruments will be enforced as of May 2018, after a two years transition period.

In the following two sections is discussed first the General Data Protection Directive (GDPR) and then the new Data Protection Directive. While the GDPR is discussed briefly, the Directive is discussed more in detail since it is directly linked with the work of law enforcement when collecting personal

[495] European Commission (2016) Joint Statement on the final adoption of the new EU rules for personal data protection, 14 April 2016, available online at: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm (last accessed:1.5.2016)
[496] Declaration 21 attached to the Treaty of Lisbon
[497] Recital 10 Directive 2016/680

data. In section 3.6.2.1 are compiled the effects that the reform package has for surveillance of individuals with non-purpose built technology.

3.6.1 Regulation 2016/679

Protection of personal data when processed in the course of activities that fall within the scope of EU law will be regulated, as of the 25th of May 2018, by Regulation 679/2016.[498] Exception to this general law make processing of personal data that does not fall within the scope of application of EU law, and especially processing of data that falls in the area of Common Foreign and Security Policy, law enforcement activities for the scope of prevention, detection, investigation and prosecution of crime and purely personal and household activities. The application of the Regulation, thus, is not completely excluded from the activity of law enforcement. It is the scope of the processing of the data to determine if the Regulation or alternatively the new Directive applies to a specific situation.

The choice for the application of the Regulation or of the Directive is relevant also in those situations in which third parties, for example service providers, retain and process data for the scope of prevention, detection, investigation and prosecution of crime and provide them to law enforcement authorities. Since in such situations the reason of the processing of the data falls within the scope of application of the Directive, the latter would apply in the concrete case. The application of the Regulation remains unaffected for all the other data processing, outside the scope of the Directive. If the third party is not bound by a legal obligation, being this a contract or another legal act, to process the data for law enforcement purposes, then its operation falls within the scope of application of the Regulation. Since this work focuses on surveillance as an activity of law enforcement in the area of prevention, detection, investigation and prosecution of crime, the application of the Regulation is as such of limited direct relevance. A few words in general about it are, however, due.

The choice for a Regulation as the legal instrument to regulate the field of data protection and repeal Directive 95/46 is not surprising. It creates the possibility for having identical rules applying in all the Member States. This facilitates the exercise of the rights for individuals, it helps for the operation of the businesses in the Digital Single Market, it prevents fragmentation in the implementation of data protection rules across the Union and it eliminates legal uncertainty. Member State law is though not completely excluded. National rules might still be adopted to further specify the application of the rules of the Regulation and sector-specific laws in areas that need more specific rules will still exist.[499]

While the distinction between the rights to privacy and data protection was not clear in Directive 95/46, the GDPR is clearly focusing only on the protection of the right to data protection, leaving out

[498] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, pp. 1–88
[499] Recital 10 GDPR

any reference to the right to privacy. The Regulation extends its territorial scope to processing of personal data taking place outside the Union territory for as long as the controller or processor are considered as established in the EU on the basis of article 3(2).

Apart the extension of the territorial scope of application, the Regulation reinforces the exercise of the rights of the individuals by introducing specific rules and conditions for the freely given consent (arts. 7-8), it facilitates the right to information and the access to the data (arts. 13-15), it codifies the so called "right to be forgotten" (art. 17),[500] it clarifies the responsibilities of the controllers and processors and holds them jointly liable in case of infringement of the rights established by the Regulation (art. 82(4)), it introduces administrative fines (art. 83), etc.

With the requirements for complying with data protection by design and by default principles (article 25) the Regulation aims to introduce data protection safeguards to be built into products and services that companies develop from the earliest stages. Backed up from administrative fines of up to 10.000.000 Euros or up to 2% of the total worldwide annual turnover of the preceding financial year (whichever is higher), this requirement might have consequences for surveillance with non-purpose built technology. The enforcement of data protection by design and by default rules might influence the design and use of non-purpose built technology by making it less attractive and more difficult for State authorities to use such devices for surveillance purposes.

3.6.2 Directive 2016/680

Directive 2016/680[501] is especially relevant for this study since it operates in the area of prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties. In the same way as the Regulation, though, it only focuses on the right to data protection leaving unregulated the protection of the right to privacy. This sub-section gives first a general description of the object and scope of application of the Directives and then it focusses on its application in cases of surveillance with non-purpose built technology and the addressing of the problems that come with this form of surveillance and that where identified in chapter 2.

In contrast to Council Framework Decision 2008/977/JHA, which it repeals, the Directive aims to introduce a level of protection of the rights of the individuals whose personal data are processed by national authorities (including law enforcement authorities) for the purposes of prevention, detection, investigation or prosecution of criminal offences and the execution of criminal penalties

[500] C-131/12 Google Spain EU:C:2014:317

[501] Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89–131

which is equivalent in the Member States.[502] The introduction of an equivalent level of protection of personal data at national level is seen to provide for an effective protection of the rights of the individuals also in those cases in which the data are exchanged among the Member States. The Directive is thus serving a double objective: i) the protection of the rights of the individuals; and ii) the facilitation of the exchange of data between Member States.

When referring to an equivalent level of protection for processing of personal data, one has to keep in mind that this refers only to a flooring level. The Directive does not provide for full harmonization of the national laws. As a result, Member States are allowed to introduce higher standards than those provided in the Directive for the protection of the rights of the data subjects.[503] There is thus the possibility that some Member States would still offer more protection than others. This should, however, not influence the exchange of data between the Member States.

The Directive protects all data subjects that fall under the jurisdiction of the Member States, thus natural persons independent of their citizenship.[504] In addition it introduces a further obligation for distinction between different categories of data subjects. These categories are: suspects, persons convicted of a criminal offence, victims and other parties (such as witnesses, persons possessing relevant information or contacts, associates of suspects and of convicted criminals).[505] The scope of such distinction and the effects that this should have for the processing of the data is, however, not explained. The Member States are left to decide by themselves the implications of the categorization of the data when implementing the Directive.

As already seen with the alternative application of the Regulation or of the Directive, the provisions of the Directive introduce obligations not only for law enforcement or other competent State authorities but also for third parties, being these public or private, that process personal data for the scope of law enforcement.[506] Under this category fall also service providers that are under an obligation to inform law enforcement authorities in case they notice suspicious behaviour of their clients. To clarify, if a third party processes data on behalf of law enforcement authorities, the Directive applies. If it does so with its own initiative, Regulation 679/2016 applies. Such a clarification on the application of the Directive is in line with international duties such as UN Resolution 17/4[507] and the Guiding principles on business and human rights.[508]

[502] Recital 7 Directive 2016/680
[503] Article 1(3) Directive 2016/680
[504] Article 1(1) Directive 2016/680
[505] Article 6 and Recital 31 Directive 2016/680
[506] Recital 11 Directive 2016/680
[507] See Resolution 17/4 adopted by the Human Rights Council on Human rights and transnational corporations and other business enterprises, 6.7.2011, para. 4
[508] See Guiding principles on business and human rights – Implementing the United Nations "Protect, Respect and Remedy" framework, annexed to the Human Rights Council Report (A/HRC/17/31) and endorsed in Resolution 17/4

The Directive reiterates the data protection principles that must guide the work of the authorities when processing personal data. The processing of personal data in accordance with the principles must be: lawful and fair; specified, explicit and for a legitimate purpose; adequate and not excessive; accurate and kept up to date when necessary; kept in a form which permits identification of the data subject for no longer than is necessary; secured from unauthorized or unlawful processing.[509] The principle of purpose limitation is, however, more flexible in specific situations.

Firstly, if personal data are processed for a purpose covered by this Directive but that is different for the purpose for which they were collected, the processing is still permitted with the fulfilling of two cumulative conditions: i) the existence of legal provisions which authorize it, and ii) the compliance with the principles of necessity and proportionality.[510]

Secondly, in recital 27 it is presented the possibility for competent authorities to process personal data collected in the context of prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected. It appears, thus, that this kind of processing is tolerated. Such a possibility shows as well the flexibility of the purpose limitation principle. This flexibility might even create the possibility for jeopardizing the principle and should thus be used carefully while introducing strict safeguards for the rights of the individuals. Furthermore, it creates the possibility for incidentally collected data to be further processed for understanding criminal activities or for making links between different criminal activities. Since there is presently not a proper protection of individuals finding themselves in incidental surveillance situations, this analysis suggests that the processing of data beyond the context in which they were collected, must exclude data collected incidentally.

For monitoring the application of the provisions adopted pursuant to the Directive and contributing to their consistent application throughout the Union, national supervisory authorities are created.[511] This authority must be independent and appointed in each Member State alternatively by the Parliament, the Government, the head of State or an independent body.[512] While the Directive applies to the activities of national courts and other judicial authorities, it does not cover the processing of personal data where courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. The same applies also for the operation of the supervisory authority. It is not competent for the supervision of processing operations of courts when acting in their judicial capacity.[513] This exemption is described as limited to judicial activities in court cases and does not apply to other activities where judges might be involved

[509] Article 4(1) Directive 2016/680
[510] Article 4(2) and Recital 29 Directive 2016/680
[511] Article 41, Recital 75 Directive 2016/680
[512] Articles 42 and 43 Directive 2016/680
[513] Article 45(2) Directive 2016/680

in accordance with MS law.[514] This would mean that the Supervisory authority can check a surveillance mandate issued by judicial authorities when this is issued outside a court case but not the collection of evidence within a judicial procedure.

Supervisory authorities have effective investigative, corrective and advisory powers. The corrective powers consist in: i) warnings to a controller or processor that intended operations are likely to infringe the provisions adopted pursuant to this directive; ii) orders to a controller or processor to bring processing operations into compliance with the provisions of the directive; and iii) the power to impose a temporary or definitive limitation on processing, including a ban. For enforcing its rights the supervisory authority has the right to bring infringements to the attention of the judicial authority by starting or being otherwise engage in legal proceedings. These however should not interfere with the specific rules for criminal proceedings, including investigation and prosecution of criminal offence, or the independence of the judiciary.[515] The bar from interference with the work of the judiciary is however limited to court cases and not to other activities of judges as for example the issuing of surveillance mandates.

The Directive introduces a right to remedies that includes the possibility to lodge a complaint with a supervisory authority or with a court, as well as the right to appeal against binding decisions of the supervisory authority before a court.[516] The individuals have also the right to be compensated for the material or non-material damages that they have suffered as a result of the operation of the law enforcement authorities operating in infringement to the law.[517]

3.6.2.1 The implications of the Directive for surveillance with non-purpose built technology

After the general discussion about the scope, objective and the reach of the Data Protection Directive, this sub-section will look into the potential implications that its provisions might present in cases of surveillance with non-purpose built technology. Collection of data from law enforcement authorities, so including those cases in which the data are collected through the means of surveillance, are covered from the provisions of this Directive that proclaims itself as designed in a technology neutral fashion in order to prevent creating a serious risk to circumvention of the protection of the rights of the individuals.[518] In chapter 2, when discussing surveillance with non-purpose built technology, three main situations that were not addressed in the existing legal framework with regards to the proper safeguarding of the rights of the individuals were identified. These are situations of incidental surveillance, mass surveillance and retroactive surveillance. The implications or not of the new Directive for each of them are discussed below in turn.

[514] Recital 80 Directive 2016/680
[515] Recital 82 Directive 2016/680
[516] Articles 52-54 Directive 2016/680
[517] Article 56 Directive 2016/680
[518] Recital 18 Directive 2016/680

i) Incidental surveillance

Incidental surveillance as such is not explicitly regulated in the provisions of the Directive. While asking a categorization of the data on the basis of the data subjects in article 6, incidentally surveilled individuals are not identified as a special category. The Directive does not clarify, thus, how to deal with data collected incidentally which have an impact for the effective protection of the rights of the individuals. This is left to be regulated at Member State level on the basis of national standards. In light of the previous analyses, this is a first point of critique to the Directive since incidental surveillance increases in cases of surveillance with non-purpose built technology.

There is though one provision in the Directive that might be interpreted as not allowing situations of incidental surveillance. Article 20 about data protection by design and default establishes that by default only data which are necessary for the specific purpose of the processing are processed. Since according to its definition in article 3(2) processing explicitly covers also the collection of data, such a provision suggests that devices that for their design collect incidental data, must not be used for surveillance. State authorities must consider the possibilities that devices used for surveillance present for incidental surveillance and adopt their decisions accordingly. Since non-purpose built technology presents often the possibility for collecting non-targeted data this must be taken into account and used in protection of the rights of the individuals.

The introduction of a Data Protection Impact Assessment (DPIA), even though plausible, is not enough for advising the authorities on the potential incidental surveillance capabilities of devices. As designed, DPIA should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of the data subject by virtue of their nature, scope or purposes.[519] In this way it covers relevant systems and processes of processing operations, but not individual cases.[520] As a result it seems more that it will operate as a risk-solutions assessment for systems of surveillance and processors and it would not influence the choice for the surveillance technology used in the specific cases. Incidental surveillance with smart meters, for example, might have different dimensions with regards to households with a single member and households with more members. In difference from Regulation 2016/679 (art. 35), in the field of prevention, investigation, detection or prosecution of crime are the State authorities and not private parties that qualify as controllers and thus are in charge of conducting the DPIA.

In cases in which the DPIA reveals a risk for the rights and freedoms of data subjects, a prior consultation of the supervisory authority is asked for. In addition, it is clear that such a DPIA focuses only on the data protection aspects of processing operations and does not cover all the aspects of the protection of the right to privacy. Such an impact assessment might serve, however, as one of the steps of an impact assessment to be used for deciding on the use of non-purpose built technology for a surveillance measure in concrete cases. This is further discussed in chapter 5.

[519] Article 27 Directive 2016/680
[520] Recital 58 Directive 2016/680

Another point of criticism to the Directive is that individuals are not informed *ex officio* on the data that have been collected about them, even though the data might not have anymore an interest for law enforcement activities. As discussed in chapter 2 this would serve as a safeguard against potential abuse from State authorities. They have though the right to request with their own initiative of being informed.[521] When the controller denies a data subject the right to information, the subject might request the national supervisory authority to verify the lawfulness of processing.[522] Even though such provisions are in general working as safeguards for the rights of the individuals, they do not work in situations of incidental surveillance in which the individual does not know about the surveillance activity and therefore does not have a reason to ask for information. The Directive does not introduce a right to be informed *ex officio*, as suggested by the Council of Europe Recommendation R87(15), but on the request of the data subject. This makes the exercise of the right difficult in those cases in which the individual is not aware that data about him are collected.

The Directive is also not introducing the right incentives for exercising the right to be informed when introducing in Article 12(4) the possibility for the processor not to respond to the request or even to charge in those cases in which someone asks often and without a basis if data about him are being processed. Such a provision has a deterrent effect in cases of mass surveillance or even incidental surveillance when individuals do not know if data about them have been collected.

In addition, where the personal data are processed in the course of a criminal investigation and court proceedings, so in cases of individual surveillance, Member States should be able to provide that the exercise of the right to information, access to, and rectification or erasure of personal data and restriction of processing is carried out in accordance with national rules on judicial proceedings.[523]

The Directive presents thus two standards.

a. In cases of data collected in the framework of prevention of crime, so outside a formal investigation or court proceedings, the data subject has a right to be informed, after his request, on the basis of this Directive.

b. In cases of criminal investigation and court proceedings, the data subject has still a right to be informed but this should be done on the basis of the national rules on judicial proceedings.

From the above one can say that the right to information according to the Directive would apply in cases of mass surveillance. In other situations, the national rules on judicial proceeding have to be taken into account. It is not clear if this would change for different categories of data subjects.

[521] Articles 12-15, Recital 40 Directive 2016/680
[522] Article 17, recital 48 Directive 2016/680
[523] Article 18, recital 49 Directive 2016/680

ii) Mass surveillance

The term "mass surveillance" is not explicitly used in the Directive which is silent on this point. This is most likely the result of the very negative attitude towards this sensitive form of surveillance that the European Parliament has taken in a number of resolutions, especially after the Edward Snowden revelations in 2013 on numerous global surveillance programs run by the NSA and the Five Eyes Intelligence Alliance. One cannot argue though that as a result of not being regulated by the Directive mass surveillance is prohibited as such. It is simply left at the discretion of national authorities, even though the principle of purpose limitation and other principles and safeguards regulated by the Directive must apply also in cases in which mass surveillance is used for the scope of preventing, investigating, detecting and prosecuting criminal activities.

With mass surveillance are not understood only large programmes of surveillance but also those situations of surveillance in which individuals are surveilled without being targeted but on the basis of the use of certain technology or their presence at specific locations. The very broad scope of crime prevention opens the doors to this form of surveillance which makes it difficult for the individuals to claim their rights in the absence of information.

In addition, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of data by Member States when carrying out activities which fall within the scope of Common Foreign and Security Policy do not fall within the scope of the Directive since they fall outside the scope of Union law.[524] The Directive thus does not offer additional safeguards for the collection of data in those cases in which law enforcement receives data collected in the framework of national security mass surveillance programmes. The possibility for such a transferral of data was pointed out from European Parliament rapporteur Morales.[525]

The Directive, though, introduces one provision that would facilitate the exercise of judicial remedies for individuals whose lives have been interfered on the basis of mass surveillance activities. This is the possibility for a data subject to mandate a not-for-profit body, organization or association to represent him in front of the courts.[526]

iii) Retroactive surveillance

[524] Recital 14, article 2(3) Directive 2016/680

[525] Working document 1, on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf, (last accessed 20.12.2013)

[526] Article 55 Directive 2016/680

In chapter 2 were discussed the effects that the time of surveillance has for the principle of presumption of innocence and for the effectiveness of the legal process. The Directive does not address the possibilities for retroactive surveillance and the implications that they have for the protection of the rights of the individuals.

Even though the Directive recognizes the importance of the principle of "presumption of innocence" in recital 31, it does this only in a passive way - with regards to the distinction of different categories of data subjects. Dynamically, the respect of the principle is linked with the different stages of an investigation and legal process and thus with the time in which surveillance is undertaken - this is not discussed in the Directive.

In addition, it is not only the possibility for retroactive surveillance that results in undermining the effectiveness of the legal process but also the possibility to use for surveillance non-purpose built devices that require processing activities which go back in time for benefiting from the collected data and for profiling the individuals. Thus, the Directive in itself does not address such a problem.

3.6.3 Concluding remarks

The new Data Protection Reform package introduces a harmonization at EU level of the protection of the right to data protection of the individuals whose private life is interfered by law enforcement authorities for the scope of prevention, detection, investigation and prosecution of crime, but does not address the protection of the right to privacy. By devoting all the legislative attention to improving rules regarding data protection it looks as if the legislator thinks that the abstract right to privacy will function better if translated in data protection language. As it was seen, however, the protection of privacy and of personal data are two separated rights and even if data protection rules are adopted and implemented in such a way that protects the right to perfection, the possibility remains for an infringement of the right to privacy.

Both the Regulation and the Directive are designed in a technology neutral fashion and do not address specifically the problems identified in situations of surveillance with non-purpose built technology – namely incidental surveillance, mass surveillance and retroactive surveillance. A reading of the Directive in a fundamental rights' light combined with technology awareness, would suggest that non-purpose built devices, since do not comply with a privacy by default approach, should not be used for collection of personal data. It is, however, for the Member States to give life to such claims in the way they will implement the rules at national level.

3.7 Discussion and conclusion

The aim of this chapter was to identify the legal framework applicable at European level which deals with privacy and surveillance and to assess if it addresses the challenges that surveillance with non-purpose built surveillance creates for the protection of the right to privacy. The attention was first drawn on the right to a protected private life contained in Article 8 ECHR and its interpretation from the European Court of Human Rights. The adoption from the Council of Europe of other legal acts on the field showed the need to extend the protection of the right to private life of the individuals to new situations that were created from the development of technology. In this context, the emergence of the right to data protection was discussed and was setting the stage for the analyses of the EU legislation that was discussed in different sections. First the focus was drawn on the Charter of Fundamental Rights that clearly distinguishes between the right to privacy and the one to data protection. The analyses of both rights clarified in how far they overlap and in how far legislation on data protection protects the right to privacy of EU citizens. The EU legislation focusing mainly on data protection was discussed under this light. Attention was paid also to the legal provisions introducing forms of interference with the life of the individuals under the former first and third pillar of the EU. The bringing together of the applicable legal framework showed two major characteristics of it: fragmentation and technology neutrality.

There is a fragmentation of the legal provisions applicable not only between the different international organisations (EU, CoE) but also within the former pillars of the EU.[527] In the area of law enforcement there are various sector-specific legislative instruments for police and judicial co-operation in criminal matters, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS), etc., which either contain particular data protection regimes, and/or which usually refer to the data protection instruments of the Council of Europe.[528] For activities within the area of police and judicial cooperation all Member States have subscribed to the Council of Europe Recommendation No R (87) 15, which sets out the principles of Convention 108 for the police sector and has become the effective standard on the issue.[529] This is not, however, a legally binding instrument.

The legislation is in general technology neutral and the use of specific technology for surveillance (being this built for that purpose or not) is not addressed neither in the laws nor in the judgments of the courts. The presence of the same level of protection has consequences especially for surveillance of citizens with non-purpose built technology since the level of intrusiveness with the life of the individuals that different technologies have is not taken into account.

[527] Brown, I., Korff, D. (2009) Terrorism and the proportionality of internet surveillance, *European Journal of criminology*, vol. 6. No. 2, 119-134

[528] COM(2010)609 final – Communication from the Commission to the EP, the Council, the ECOSOC and the CoR – A comprehensive approach on personal data protection in the European Union

[529] Korff, D. (2014) The rule of law on the internet and in the wider world, *Issue Paper published by the Council of Europe Commissioner for Human Rights*, available online at: https://wcd.coe.int/ViewDoc.jsp?id=2268589 (last accessed: 1.11.2014), p. 113

Surveillance with non-purpose built technology can have the form of direct surveillance or dataveillance via the data collected by the devices and systems that we use. It was seen that interference with the private life of the individuals in these cases might fall simultaneously under the privacy and the data protection regime and that data protection rules might also play a role for the protection of privacy. Even if for the Charter of Fundamental Rights of the EU the right to privacy and data protection are presented as separate rights, the historic evolution of the right to data protection from the one to privacy in the Council of Europe context projects itself often in a confusion in the use of the terminology both from the doctrine and from the jurisprudence alike.

While at Council of Europe level, the legal instruments, albeit with non-binding force, give clear messages to the Member States to use certain safeguards, as for example: a) the limitation of the purpose of the data collected; b) the same level of protection for content and metadata; c) a limitation of the police interference with the rights of individuals in case of necessity to the prevention of real danger or the suppression of a specific criminal offence, etc., the same is not clearly regulated in EU provisions. Furthermore, the possibility to retain and use data collected for other purposes for law enforcement purposes opens the gates to mass surveillance with non-purpose collected data. For the CJEU that invalidated the Data Retention Directive the scale of surveillance and the change of the purpose of the collected data was not by itself a sufficient reason for the invalidation of the Directive. It had to be assessed together with the safeguards for the data access and the requirements for service providers.

Surely, CJEU decisions on the validity of legislative measures at EU level reflect the separation of powers between the judiciary and the legislative, and as a result the courts in general are inclined to invalidate legislative measures only for sufficiently serious breaches of the laws. Therefore, the main role for ensuring the compatibility of legislation with fundamental rights of the citizens must be with the legislator itself. This is reflected also in a communication of the Commission of the European Union requiring all new legislative and major policy-defining proposals to be checked for compliance with the Charter of Fundamental Rights, including the rights to privacy and data protection.[530] All the Commission departments have a duty to check not only their legislative proposals but also to monitor the work of the two branches of legislative authority in order to determine compliance with fundamental rights.[531] This did not bar the Commission, however, to bring through and even try to enforce[532] the (now invalidated) Data Retention Directive. At EU level, therefore, not only the legislation is not designed to properly protect citizens in cases of State surveillance with technology not built for the purpose of surveillance, but, as in the case of the Data Retention Directive, there is the risk to adopt legislation that introduces some form of surveillance without the proper safeguards.

[530] COM(2005)172 on compliance with the Charter of Fundamental Rights
[531] See para. 5 and para. 28 COM(2005)172
[532] See application of the Commission in case C-329/12 Commission v. Germany, withdrawn after the invalidation of the Data Retention directive with the Court Order of 5 June 2014

The entry into force of the Lisbon Treaty and the elimination of the pillar structure of the EU, and in particular the introduction the new legal basis on data protection in Article 16 TFEU, allow the establishment of a new and not fragmented data protection framework for the protection of personal data,[533] whilst respecting the specific nature of the field of police and judicial cooperation in criminal matters.[534] In particular, it allows the revised EU data protection framework to cover both cross-border and domestic processing of personal data.[535]

The legal basis of Article 16 TFEU covers however only the adoption of data protection rules and does not extend to the protection of the right to privacy of the individuals. This is reflected also in the new data protection reform package. The protection of the right to privacy remains highly guided from the Article 8 ECHR and the elaboration of the right by the Court of Justice decisions and the test to identify arbitrary state interferences established by the Court of Human Rights. Data protection rules, as already seen, will protect the right to privacy only in those cases in which non-compliance with data protection standards amounts to an infringement of the right to information privacy of the citizens. Otherwise the right of privacy in itself is insufficiently safeguarded.

The EU's new reformed data protection package will be enforced as of May 2018. As already stated, it focuses exclusively on the protection of the right to data protection leaving unregulated the right to privacy. Directive 2016/680 focuses on the operating of law enforcement but it fails to bring together the fragmented legislation that exists in the area of police and criminal cooperation at EU level. At the same time, it has the advantage to apply not only when information is being exchanged between the Member States but also when they process the data domestically. The technology neutral nature of the legislation makes surveillance with purpose built as well as non-purpose built technology fall under the same rules and safeguards. It was seen, however, that the specific problems identified in cases of surveillance with non-purpose built technology are not addressed by the legislation.

In conclusion, it can be said that while the legal framework contains a number of laws on exchange of data relevant for law enforcement purposes among the Member States and the EU bodies, it does not harmonize the way surveillance is performed. Furthermore, while the legislator has been taking over the task of regulating at European level the right to data protection, the protection of the right to privacy is left in the hands of the judiciary and the trust in the proper application of the proportionality principle. However, from the study of the legal framework a number of insight and principles can be identified that can be used and would assist for protecting the right to privacy of

[533] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century

[534] See Declarations 20 and 21 following the Treaty of Lisbon

[535] Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29(2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

the individuals from the challenges that surveillance with non-purpose built technology presents. Any law enforcement interference with the private life of the individuals must, for example, comply with the principle of proportionality, must not go further than what is strictly necessary and must be supervised under a system of prior authorization. Individuals must be informed about the collection of their persona data which is done under a continuous system of checks and balances. The introduction of rules that change the purpose of the data collected must be assessed both in light of data protection and privacy concerns. In addition, and this is particularly important in cases of surveillance with non-purpose built technology, technology that does not comply with the privacy by design and by default criteria must not be used for surveillance.

Chapter 4 Surveillance with non-purpose built technology – Case studies

4.1 Introduction

This chapter has a dual aim. The first aim is to present and analyse concrete examples of non-purpose built technology that is used or that has a potential to be used by law enforcement for surveillance purposes. The second aim, very closely related to the first one, is to test in concrete cases the relevance of the challenges to the right to privacy that were identified in chapter two. Since in the previous chapter it was concluded that the current legal framework does not address the identified challenges satisfactorily, the case studies will show the relevance of these persisting challenges. The three chosen case studies are: smart meters,[536] smart phones and stand-alone GPS navigation devices. The reasons for choosing these case studies are briefly explained below.

The decision to assess smart meters as a case study representing non-purpose built technology that can be used for surveillance is not arbitrary and is supported by a number of reasons. Firstly, smart meters are certainly not built for the purpose of surveillance, but as it will be argued in the following section they present possibilities and potential to be used for such a purpose. They clearly qualify, therefore, under the definition of non-purpose built technology that can be used for surveillance. Secondly, the definition of "private life" embedded in article 8 ECHR is covering 4 large areas of personal autonomy: private life, family life, home and correspondence. Smart meters are seen in this study as interfering with 3 of these areas of personal autonomy. They are installed in households detecting activities taking place within their walls and interfere as a result with the inviolability of the home as well as with the private life and the family life of its occupants. Thirdly it is the European Union that has imposed on the Member States the obligation to substitute at least 80% of the electricity meters with smart ones till the year 2020. Individuals in a number of Member States are therefore obliged to allow the introduction of these devices in their households as a legal obligation which, on the other side, creates the possibility for infringing their fundamental rights. The way that smart meters operate, their introduction in many households within the EU on the bases of broad energy saving programmes and the ability that they have for spying activities taking place within private premises makes them an ideal case study for non-purpose built but surveillance ready technology.

A discussion on non-purpose built devices with a potential to be used for surveillance cannot be complete without a discussion on smartphones. There are various reasons that justify such a choice. Firstly, smartphones are not built for the purpose of surveillance but they make surveillance

[536] It has to be noted that for the scope of this study are considered only smart meters that measure the consumption of electricity and not of water or gas. In addition, also the use of the term "energy" is limited to electric energy and does not cover gas or other forms of energy.

ubiquitous and are a goldmine for law enforcement authorities enabling them to access valuable information.[537] Secondly, smartphones combine in one device different ways of communication. Individuals have the possibility to communicate in traditional ways, as for example with voice communication, sending short text messages (sms), or in new ways via internet messenger services, e-mailing, chatting, etc. Surveillance with smartphones would thus interfere with the privacy of communications as the forth area of personal autonomy explicitly included in article 8 ECHR. Thirdly, the popularity of these devices has quickly outnumbered feature phones[538] in Europe.[539] Smartphones have turned from a status symbol to a necessity for their users and they represent the source of most of the internet trafficking.[540] These devices combine features of mobile phones with advanced computing capabilities which makes them important portable data carriers. Due to these capabilities smartphones are a good example showing how one device might give the possibility for interfering with different set of data. Apart communication, the computing capabilities of smartphones create the possibility for interfering also with other aspects of the private life, as it is possible for example via location tracing, video and image capturing, etc.

The third case study is dedicated to stand-alone GPS navigation devices that interfere with the privacy of location and space. Many devices are nowadays furnished with GPS technology which may go two ways. It facilitates on one side decisions on travel itineraries with the scope of reaching locations and on the other side the tracing of the device for different reasons, including potential assistance for vulnerable persons.[541] Some examples of devices which have built-in GPS technology as a basic feature are: smart phones, smart bike locks, smart watches, some digital cameras, etc. Although all the devices mentioned above might have an interest to be used by law enforcement for surveillance purposes, this study focuses on standalone portable GPS navigation devices that are used by drivers to facilitate their navigation. These devices help drivers to reach a specific destination, to stay within the road speed limits, to access traffic news, to locate points of interest, etc. This choice is justified by different reasons.

Firstly, these devices are not built for the purpose of surveillance but have a potential to be used for such a purpose since they provide location as well as movement data. Black boxes, or event data recorders as they are officially called, are excluded from the scope of this chapter even though their installation in new cars is nowadays almost a standard. This exclusion is linked with the purpose of these devices. Black boxes are designed to collect evidence for facilitating the work of law

[537] Coudert, F., Gemo, M., Beslay, L., Andritsos, F. (2011) Pervasive Monitoring: Appreciating Citizen's Surveillance as Digital Evidence, in *Legal Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention* (ICDP 2011), pp. 1–6

[538] The term "feature phone" is used for referring to a category of mobile phones that can be considered nowadays as outdated since it lacks the technology advantages of smart phones

[539] Arthur, C., Garside, J. (2011) Smartphones take lead in European mobile phone market, *The Guardian*, 8 September 2011, available online at: http://www.theguardian.com/technology/2011/sep/08/smartphones-take-lead-in-mobile-phone-market (last accessed:20.1.2016)

[540] Bigo, D. et al. (2014) Study on the National programmes for mass surveillance of personal data in the EU Member States and their compatibility with EU law

[541] Karim, W. (2004) The privacy implications of personal locators: Why you should think twice before voluntarily availing yourself to GPS monitoring, *Journal of Law and Policy, vol. 14, pp. 485-515*

enforcement and insurance companies in cases of events or accidents.[542] As a result, they do not fully satisfy the definition of non-purpose built technology used for surveillance. Secondly, privacy of location and space, even though not explicitly mentioned in article 8 ECHR, is one of the newest areas with which the projection of the private sphere of the individuals as well as its protection are enlarged as a result of the development of technology.[543] The right to privacy does, as it was already seen in chapter 3, protect individuals and not spaces thus the notion of privacy of location and space has to be understood as protecting a particular space not because of its existence but for being linked to an individual. The protection of this area of the individuals' private sphere gives him the right to determine for himself to what extent information on his location and movements is communicated to others.[544] Thirdly, the choice of GPS navigation devices as a case study will also allow us to discuss the problems of privacy invasion in the public space.

In chapter 2, incidental surveillance, mass surveillance and retroactive surveillance were identified as the main challenges that surveillance with non-purpose built technology creates for the right to privacy. In this chapter these challenges are used as a framework of analyses and each case study is tested in light of the potential for creating situations of incidental surveillance, mass surveillance and retroactive surveillance. It is accepted that different technologies might present additional challenges to the protection of the right to privacy. In this light the framework of analyses is not static. In the case of smartphones also the proportionality of using for surveillance purposes a device that gives the possibility to access different sets of data is discussed together with the set framework. In the case of stand-alone GPS navigation devices are discussed also the challenges that derive from interference with the life of individuals in those cases in which their activities take place in public. For avoiding any conviction bias, the technology itself and its actual or potential use for surveillance purposes are reviewed first. Afterwards the challenges presented to the right to privacy are discussed.

After this short introduction follow three sections dedicated to each of the case studies. Section 4.2 elaborates on smart meters, section 4.3 on smart phones and section 4.4 on stand-alone portable GPS devices. The aim is to see the effects for the protection of the right to privacy that the use of these devices for surveillance has in the current EU legal framework. The conclusions are presented in section 4.5.

4.2 Smart meters

The potential use of smart meters from law enforcement authorities for surveillance purposes is the first of the analysed case studies. The section does not have the aim to discuss the general problems

[542] Chae, K., Kim, D., Jung, S., Choi, S., Jung, S. (2010) Evidence collecting system from car black boxes, in *Proceedings of the 7th IEEE conference on Consumer communications and networking conference*, pp. 254-255
[543] Wright, D., Raab, C. (2014) Privacy principles, risks and harms, *International review of law, computes and technology*, vol. 28, no. 3, pp. 277-298
[544] Duckham, M., Kulik, L. (2007) Location privacy and location-aware computing, in Drummond, J. et al. eds., *Dynamic and Mobile GIS: Investigating Changes in Space and Time*, pp. 35-52

that smart meter data create for the protection of the rights to privacy and data protection of European citizens. The literature on privacy and data protection has already attributed substantial interest to this and related topics.[545] The section contributes to the existing literature by focusing on the problems that the use of smart meters by law enforcement authorities for surveillance purposes creates for safeguarding the right to privacy of European citizens in the current European legal framework in light of the previous theoretical elaboration.[546]

In sub-section 4.2.1 is presented some background information on the introduction of smart meters in the European Union and on their operation. In sub-section 4.2.2 is analysed the nature of smart meter data and these data are qualified under the framework of data protection and privacy rules. In sub-section 4.2.3 on the basis of scientific studies are presented examples of data and information that can be retrieved by smart meters. The aim of this sub-section is to present situations in which smart meter data might be relevant for surveillance and for law enforcement authorities. In sub-section 4.2.4 the theoretical challenges that surveillance with non-purpose built technology creates for the right to privacy of the individuals are assessed for the case of smart meters. In sub-section 4.2.5 is analysed the applicable EU legal framework and are presented practical suggestions to safeguard the right to privacy of European citizens in the presence of surveillance via smart meters. The concluding remarks are presented in sub-section 4.2.6.

4.2.1 Background information on smart meters in Europe

Smart meters are introduced in the European Union because of the contributions they are expected to make towards the energy saving targets aimed by the Member States.[547] The European legislator set to the Member States the target of substituting at least 80% of the electricity meters in their countries with smart ones until the year 2020.[548] After a high speed starting in some Member States (as for example Sweden, Finland and Italy that already finalised their nationwide smart metering roll-outs)[549] the introduction of smart meters has faced in other Member States concerns that were not

[545] See for example: Knyrim, R., Trieb, G. (2011) Smart metering under EU data protection law, *International Data Privacy Law*, vol. 1, no. 2, pp. 121-128; Savirimuthu, J. (2013) Smart meters and the information panopticon: beyond the rhetoric of compliance, *International Review of Law, Computes & Technology*, vol. 27, no. 1-2, pp. 161-186; Zeadalli, S., Pathan, A.-S., Alcaraz, C., Badra, M. (2013) Towards privacy protection in smart grid, *Wireless Personal Communication*s, vol. 73, pp. 23-50

[546] Part of this research is already published in: Milaj, J., Mifsud Bonnici, J.P. (2016) Privacy Issues in the Use of Smart Meters—Law Enforcement Use of Smart Meter Data, in Beaulieu, A., de Wilde, J. and Scherpen, J. (eds.), *Smart Grids from a Global Perspective: Bridging Old and New Energy Systems*, pp. 179-196; and Milaj, J., Mifsud Bonnici, J.P. (2016) Smart meters as non-purpose built surveillance tools, in Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (eds.), *Privacy Technologies and Policy,* pp. 81-95

[547] See Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC, OJ L 114, 27.4.2006, article 13; Commission staff working document (2014) Cost-benefit analyses & state of play of smart metering deployment in the EU-27 - Accompanying the document Report from the Commission Benchmarking smart metering deployment in the EU-27 with a focus on electricity /* SWD/2014/0189 final */

[548] See Annex I, para. 2 of Directive 2009/72/EC

[549] Covrig, C.F., et al (2014) Smart Grids Projects Outlook, available online at: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf, (last accessed: 29.4.2015) p. 89; Lo Schiavo, L., Delfanti, M., Fumagalli, E., Olivieri, V. (2013) Changing the Regulation

considered before, among which privacy and data protection challenges (as for example in the Netherlands and in Germany).[550]

A key feature of smart meters is the collection and communication of energy consumption data[551] between the meter and other parties. These other parties can be service providers,[552] consumers of energy, or even independent service providers that facilitate the communication between consumers and the meter.[553] The detailed data communication is said to benefit not only the service providers and energy companies (learning in quasi real time about specific energy demand and enabling companies to enhance the accuracy of their long term energy demand predictions which would impact their production and purchasing strategy) but also the consumers (that will have an accurate overview on their consumption and might change their consumption behaviour in accordance with electricity fees).[554]

It is to be highlighted that smart meters transfer data on the usage of energy and not just final energy consumption data. A number of studies have shown the interest of actors other than electricity supply companies for these data. This interest might be for engaging in illegal, commercial, law enforcement or other activities. Smart meter data for illegal activities can be used for example by burglars who are interested to learn when a residence is unoccupied, or by stalkers seeking to track the movements of their victim.[555] Other actors might have a commercial interest in the use of smart

---

for Regulating the Change - Innovation-driven regulatory developments in Italy: smart grids, smart metering and e-mobility, *Energy Policy*, vol. 57, pp. 506-517; Zhou, L., Xu, F.-Y., Ma, Y.-N. (2010) Impact of smart metering on energy efficiency, Proceedings of ICMLC 2010 International conference, vol. 6, pp. 3213-3218

[550] Cuijpers, C., Koops, B.-J. (2012) Smart metering and privacy in Europe: Lessons from the Dutch case, in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds.), European data protection: Coming of age, Springer, pp. 269-293; Pallas, F. (2012) Beyond gut level – Some critical remarks on the German privacy approach to smart metering, , in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds.), European data protection: Coming of age, Springer, pp. 313-345; Alabdulkarim, L., Lukszo, Z. (2011) Impact of privacy concerns on consumers' acceptance of smart metering in the Netherlands, *IEEE*, pp. 287-292

[551] European Commission (2011) A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the Smart Meter

[552] The term "service providers" used in this chapter covers distribution system providers, transmission system providers or other parties that receive data directly from smart meters, depending from the organization of the electricity distribution system in each Member State

[553] See for example the scheme of operation of smart meters in the Netherlands: Boekema, J. (2011), TNO Report - Assessment of the implementation regulations for Smart Meters, available online at: https://www.tno.nl/media/1050/assessment-of-the-implementation-regulations-for-smart-meters.pdf, (last access 16.7.2015), p.13; Helburg, H., van (2014), RVO Report - Dutch Energy Savings Monitor for the Smart Meter, available online at: http://english.rvo.nl/sites/default/files/2014/06/Dutch%20Smart%20Meter%20Energy%20savings%20Monitor%20final%20version.pdf, (last access 16.7.2015), pp. 44-48

[554] Faraqui, A., Harris, D., Hledik, R. (2010) Unlocking the €53 billion savings from smart meters in the EU: How increasing the adoption of dynamic tariffs could make or break the EU's smart grid investment, *Energy Policy*, vol. 38, n. 10, pp. 6222-6231

[555] Lisovich, M., Mulligan, D., Wicker, S. (2010) Inferring personal information from demand-response systems, *IEEE Security and Privacy*, pp. 11-20, Cavoukian, A., Polonetsky, J., Wolf, C. (2010), Smart privacy for the smart grid: embedding privacy into the design of electricity conservation, available online at: https://www.privacybydesign.ca/index.php/paper/smartprivacy-for-the-smart-grid-embedding-privacy-into-

meter data to target advertising of special products to identified households or even to individual inhabitants (e.g. more efficient energy saving devices).[556] Among the other interested actors have been cited law enforcement authorities,[557] insurance companies, parties in a civil litigation, landlords, the press, or also simply the cohabitants of a household spying on each other.[558] The interest of law enforcement authorities in smart meter data is discussed further in sub-section 4.2.3.

The communication of the energy consumption related data from smart meters is said to create accurate maps of the activities taking place within a household. As stated by Martin Pollock[559] from Siemens Energy: "*We, Siemens, have the technology to record it (energy consumption) every minute, second, microsecond, more or less live…. From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data*."[560]

4.2.2 Smart meter data under data protection and privacy rules in Europe

As explained in the previous section, smart meters have the capability to surveil the life of the consumers of electricity. To assess the effects that surveillance via these devices has for the right to privacy and data protection of European citizens, it is important to first establish if smart meter data fall under the protection offered by the applicable EU rules. The aim of this sub-section is to analyse the nature of smart meter data and to examine if they could be qualified under the EU framework of data protection and privacy rules.

---

the-design-of-electricity-conservation/ (last access 15.4.2015); Quinn, E.L. (2008) Privacy and the new energy infrastructure, *CEES Working Paper no. 09-0001*, pp. 41, McDaniel, P. (2009) Security and privacy challenges in the smart grid, *IEEE Security and Privacy*, vol. 7, pp. 75-77, Lerner, J.I., Mulligan, D.K. (2008) Taking the long view on the fourth amendment: Stored records and the sanctity of the home, *Stanford Technology Law Review*, vol. 3, pp. 13; Subrahmanyan, P.A. (2005) Network security architecture for demand response/sensor networks, Report for the California Energy Commission, Public Interest Energy Research Group, available online at: http://www.law.berkeley.edu/files/demand_response_CEC.pdf (last accessed: 15.4.2015)

[556] McKenna, E., Richardson, I., Thomson, M. (2012) Smart meter data: Balancing consumer privacy concerns with legitimate applications, *Energy Policy*, vol. 41, pp. 807-814; Anderson, R., Fuloria, S. (2010) On the security economics of electricity metering, in *Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS 2010)*, pp. 18, Bohli, J., Sorge, C., Ugus, O. (2010) On the security economics of the electricity metering, *Proceedings of 2010 IEEE International Conference on Communications Workshops*, pp. 10

[557] See European Commission, Smart Grid Task Force 2012-2014, Expert Group 2, Data protection impact assessment template for smart grid and smart metering systems, available online at: https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf (last accessed 4.1.2016), p. 5

[558] Quinn, E.L. (2008) Privacy and the new energy infrastructure, *CEES Working Paper no. 09-0001*, pp. 41; Hargreaves, T., Nye, M., Burgess, J. (2010) Making energy visible: A quantitative field study of how households interact with energy from smart energy monitors, *Energy Policy*, vol. 38, pp. 6111-6119

[559] Director of metering services at Siemens Energy

[560] Wynn, G. (2010) Privacy concerns challenge smart grid rollout, Reuters 25 June 2010, available online at: http://www.reuters.com/article/2010/06/25/energy-smart-idUSLDE65N2CI20100625 (last accessed: 13.5.2015)

As already discussed in chapter 3, the right to data protection in the EU focuses on the fair and legitimate collection and processing of personal data and is mainly governed by article 8 of the European Charter of Fundamental Rights, article 16 TFEU, Directive 95/46/EC[561] and a number of other provisions contained in secondary legal sources.[562] Data protection is often seen in the literature as a tool that insures the transparency of the operation of different institutions or bodies that act as data controllers. Its regulation aims at the creation of a clear framework for collection, storage and use of personal information and facilitates data processing activities while providing a set of safeguards for the citizens.[563]

Privacy on the other side aims to protect the private life of the individuals from arbitrary interferences of State actors. Even though no clear definition of what is covered with the term 'private life' exists and this is to be established on a case by case basis, it appears clear that private life includes many aspects such as: (i) privacy of the person, (ii) privacy of personal behaviour,[564] (iii) privacy of personal communication, (iv) privacy of personal data,[565] (v) privacy of location and space, (vi) privacy of thoughts and feelings,[566] and (vii) privacy of association. As it was already seen, in the EU the right to privacy is mainly regulated by article 7 of the European Charter of Fundamental Rights and a major role in its protection plays also article 8 of the European Convention of Human Rights and the case law decided on its basis.[567]

Even though from the Charter articles the separation between the rights to privacy and data protection seems normatively clearly defined, as discussed in chapter 3, one has to keep in mind that

[561] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995

[562] See for example: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31/07/2002; Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001; Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385/1, 29.12.2004

[563] Gutwirth, S., De Hert, P. (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, pp. 61-104

[564] Kalogridis, G., Denic, S.Z. (2011) Data mining and privacy of personal behavior types in smart grid, in *IEEE*, pp. 636-642

[565] The difference and interlink between privacy and data protection are discussed in chapter 3 of this study

[566] See for example the newest developments on wireless brain–computer interface in Borton, D.A. et al. (2013) An implantable wireless neural interface for recording cortical circuit dynamics in moving primates, *Journal of Neural Engineering*, vol. 10, no. 2, pp. 16; Young, S. (2013) A wireless brain-computer interface, available online in: http://www.technologyreview.com/news/512161/a-wireless-brain-computer-interface/, (last accessed 24.04.2013)

[567] On the definition of the term "private life" see for example: Niemietz v. Germany, ECHR application no. 13710/88, 16 December 1992, para. 29; Peck v. The United Kingdom, ECHR application no. 44647/98, 28 January 2003, para. 57; Pretty v. The United Kingdom, ECHR application no. 2346/02, 29 April 2002, para. 61

due to the historical emergence of the right to data protection from the one to privacy,[568] their distinction is not always clear in the doctrine and the case law of the European Court of Justice. This confusion between the two rights is also due to the fact that despite being separate, [569] data protection and privacy often overlap with each other. This can be seen, for example, in the invalidation of the *Data Retention Directive* case were the Court of Justice of the EU clearly stated that the retention of personal metadata from electronic communications translates in an interference with the private sphere of the individuals, therefore with the right to privacy.[570] The private information obtained and the interference with the private life caused by the provisions of the Directive was the result of the processing of personal data.

From the above elaboration, it is clear that interference with personal data might interfere both with the right to data protection and the right to privacy of the individuals. To be able to qualify the effects of the data collected by smart meters under the rights of privacy and data protection we would therefore first need to assess if these data qualify as personal data.

4.2.2.1 Smart meter data as personal data

The current EU legal framework for smart meters is composed of Directive 2009/72/EC (Energy Internal Market Directive),[571] and Directive 2004/22/EC (Measuring Instrument Directive).[572] These directives regulate insufficiently the protection of privacy and personal data. Other provisions in the field have the form of soft law recommending rather than requiring the application of safeguards for the protection of the rights to privacy and data protection.[573] These soft laws direct, however, the attention to the respect of the general legal regime in the field, already suggesting in this way the application of the general data protection rules.

Personal data are defined in Directive 95/46/EC article 2(a) as any information relating to an identified or identifiable natural person. An identifiable person is further defined as him who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. The

[568] For a historical view into the development of the right to data protection in the EU see: Mayer-Schoenberger, V. (1997) Generational development of data protection in Europe, in Agre, P.E., Rotenberg, M. (eds.), *Technology and Privacy: The new landscape*, pp. 219-238

[569] Friedl v. Austria, ECHR application 15225/89, 31 January 1995. In this case the fact that someone was photographed in a manifestation by the police, but was not identified, was not considered as a violation of his right to a protected private life but it was still qualified as falling in the field of data protection.

[570] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 27

[571] Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, OJ L 211, 14.8.2009

[572] Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments, OJ L 135, 30.4.2004

[573] Commission Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems, OJ L 73, 13.3.2012, para. 4-9; Commission Recommendation 2014/724/EU of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, OJ L 300, 18.10.2014

same definition is included also in the new Data Protection Regulation 2016/679, article 4(1) and Directive 2016/680, article 3(1), though the number of identifiers has increased: "…*in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

It is true that smart meter data give information on the energy consumption but at the same time domestic activities are revealed on the bases of the energy usage of electric appliances in a household.[574] Information on electricity consumption gives direct information on the habits of the members of the household, as for example the times when they are at home, if they have healthy habits (e.g. cooking regularly or using largely the microwave for convenience food), if they spend time together or in separate rooms, the activities they perform and even sensitive information (e.g. the use of medical devices).[575] Below we will establish if the electricity consumption data is related to identified or identifiable members of the household and therefore qualifies as personal data.

Often in policy papers and the doctrine smart meter data are referred to as personal data,[576] however legally it is not clear if they fall within the definition of personal data. There are different opinions as to the data subjects with whom these data are linked. These are: (a) the member of the household that is the signatory of the electricity supply contract; (b) all the members of the household as a group; or (c) each individual member of the household. We will discuss each of these prepositions in turn.

For the Article 29 Working Party a domestic consumer of energy is associated with unique identifiers that are inextricably linked with the member of the household who is responsible for the account. The device enables that an individual is singled out from other consumers.[577] This qualification would comply with the definition of personal data relating all the data received from a smart meter with the individual responsible for the account. From a human rights' point of view, however, we find this qualification as problematic since it attributes to one member of the household all the generated electricity data, even for periods of time in which it can be proven that the individual was not present at the location.

[574] Weiss, M., Helfenstein, A., Mattern, F., Staake, T. (2012) Leveraging smart meter data to recognize home appliances, in *Proceedings of IEEE Pervasive Computing and Communication PerCom*, pp. 190-197
[575] Kalogridis, G., Denic, S. (2011) Data Mining and privacy of personal behavior types in smart grid, in *Proceedings of the 11th IEEE International Conference on Data Mining Workshops*, pp. 636-642
[576] EDPS (2012) Opinion of the European Data Protection Supervisor on the Commission Recommedation on preparations for the roll-out of smart metering systems; Cuijpers, C., Koops, B.J. (2012) Smart metering and privacy in Europe: Lessons from the Dutch case, in Gutwirth, S., Leenes, R., de Hert, P. (eds.), *European data protection: Coming of age*, pp. 269-293
[577] Article 29 Data Protection Working Party (2011) Opinion 12/2011 on Smart Metering, 4.4.2011

In contrast to the opinion of the Article 29 Working Party, Knyrim and Trieb (2011) suggest that the Directive's definition of personal data should be interpreted broadly in line with some national data protection laws. They present the example of Austria that in its implementation of the Directive refers to personal data as linked not only to a single person but also to a 'community of persons'.[578] With this broad interpretation the definition of personal data would allow for "groups of individuals" to qualify as "identified or identifiable" data subjects.[579] This idea is supported also by King and Jessen (2014) that plead for the adoption of a more inclusive definition of the data subject which would cover a group of natural persons living together in a household, including temporary guests.[580]

It is easy and automatic to link smart meter data just to the person that has signed the contract with the service provider or to refer to a community of persons instead, even though the latter might create problems with regards to the consent needed in cases in which the data subject would allow access to the data by third parties. We do not agree with these simplistic views. As stated in an opinion of the European Data Protection Supervisor (EDPS) the long period of retention and the possibility of profiling while linking different databases gives the possibility to separate the data and link them to the individually identified or identifiable members of the household in line with the definition of personal data: "*Profiles can thus be developed, and then applied back to individual households and individual members of these households*".[581] In line with this opinion we submit that smart meter data are personal data and they are linked with individual household members. Of course, this would require some profiling activity. This does not mean, however, that smart meter data would qualify as personal data only after their analyses and attribution to individual members of the household. As stated in the definition of personal data, they qualify as such for belonging to an identified or identifiable person. Smart meter data are related with identifiable individuals from the moment they are collected.

Qualifying smart meter data as personal data brings them into the realm of application of the EU data protection legislation with regards to the collection and processing of the personal data. As already seen in the Data Retention Directive case, the collected and processed personal data create the possibility to interfere with the private sphere of the individuals concerned.[582] Just from the few examples mentioned above the data collected with smart meters give information on different aspects of the private life of the citizens as for example: privacy of behaviour, privacy of data, privacy of association (learning about the presence of guests and how often) and even privacy of the individuals´ body (since it is possible to detect sensitive information as for example medical appliances at home and how often they are used). It thus interferes at the same time with the private

[578] Datenschutzgesetz 2000, Bundesgesetz über den Schutz personenbezongener Daten, § 4(3)
[579] Knyrim, R., Trieb, G. (2011) Smart metering under EU data protection law, *International Data Privacy Law*, vol. 1, no, 2, pp. 121-128
[580] King, N.J., Jessen, P.W. (2014) Smart metering systems and data sharing: why getting a smart meter should also mean getting strong information privacy controls to manage data sharing, *International Journal of Law and Information Technology*, pp. 1-39
[581] EDPS (2012) Opinion of the European Data Protection Supervisor on the Commission Recommendation on preparations for the roll-out of smart metering systems, para. 18
[582] Savirimuthu, J. (2013) Smart meters and the information panopticon: beyond the rhetoric of compliance, *International Review of Law, Computes & Technology*, vol. 27, no. 1-2, pp. 161-186

life of the individuals, the inviolability of the home and the family life. In the following section, is presented the relevance that information retrieved via smart meter data has for law enforcement authorities.

4.2.3 Smart meter data for law enforcement authorities

As already stated earlier in this section, smart meter data present interest for different actors, law enforcement authorities being one of these. They can have direct access to the data, via the smart meter device, or receive the information from the service providers or other parties that have access to the data. The aim of this sub-section is to present a number of possibilities that smart meters offer for collecting data and information on the activities that individuals perform within the privacy of their homes and not only, as well as on the relevance that these data might have for law enforcement authorities.

The use of data from electricity measuring devices for law enforcement purposes is not a new phenomenon.[583] The so-called "dumb" or analogue meters (i.e. traditional electricity meters that are not smart and are still present in those households that have not yet installed smart ones) give information on the total consumption of energy in the households and the possibility for readings of the data in monthly or longer time intervals. Law enforcement authorities are already making use of these data and in certain cases have even regarded very high electricity consumptions as an indicator that certain illegal activities (such as the cultivation of illegal narcotic plants) are performed in the household. Smart meters on the other side give much more detailed data.[584] These data are linked with the usage of different (identifiable) devices and give the possibility to draw accurate maps of the activities that take place within a household. The possibilities of smart meters for collecting data on what happens within the walls of a household, detecting activities and disclosing them to the outside world are, therefore, broad and accurate. These devices give the possibility for detecting illegal activities, for verifying defendants' claims,[585] suspects' claims and even for creating and verifying profiles of certain criminals as for example sex offenders (e.g. paedophiles).

The frequency of the communicated data discloses not only the presence of electric devices and their on or off status but shows also activities that members of a household do within the privacy of their home. The analyses of energy usage over long periods of time may show also patterns of use and even distinguish situations that are outside the normal every day routine, as for example the

[583] Balough, C.D. (2011) Privacy implications of smart meters, Chicago-Kent Law Review, vol. 86, no. 1, pp. 161-191

[584] Jones, K.B., Zoppo, D. (2014) A smarter, greener grid, Praeger, p. 26

[585] Lisovich, M., Mulligan, D., Wicker, S. (2010) Inferring personal information from demand-response systems, IEEE Security and Privacy, pp. 11-20

presence of guests.[586] Data can assess sleeping times, working times, if someone is at home, when the family goes on holidays, etc.

The type of devices within a household and their status are not the only details that one might learn from smart meter data analyses. Some studies present the possibility for disclosing even the television programmes that one watches.[587] Apparently, "*the amount of light and dark emitted on the display for individual frames is unique for each TV program and movie*" and gives the possibility to identify the watched program at any particular point in time. Studies show that also the copyright protection or its absence of a DVD that is played can be detected.[588] In addition data from charging of electric cars would give information on the kilometres travelled and combined with other information might validate also other information on the destinations reached.[589]

From the above possibilities that smart meter data create, one might imagine all the interesting information that law enforcement authorities would be able to deduce by using these devices and the data they collect for surveillance. This information would facilitate the creation of detailed profiles of the members of a household and especially of suspected individuals under formal inquiry or not – since the data show patterns of their routine life, behaviour and preferences.

The frequent communication between the smart meter and the service provider in short time intervals of 15 minutes (even though shorter time intervals are not excluded)[590] would also give the possibility to use this feature of the system for direct surveillance of the members of the household. One can learn about their presence at home or if they use the electricity for illegal activities (as in the example of the cultivation of narcotic plants, unlicensed commercial activities, sweatshops, etc.). The problem that the frequent access to energy consumption data creates for the right to privacy and

[586] Kim, Y., Schmid, T., Srivastava, M., Wang, Y. (2009) Challenges in resource monitoring for residential spaces, in *Proceedings of the first ACM Workshop on Embeded Sensing Systems for Energy-Efficiency in Buildings*, pp. 1-6

[587] Mills, E. (2012) Researchers find smart meters could reveal favorite TV shows, *CNet News,* 24 January 2012, available online at: http://news.cnet.com/8301-27080_3-57364883-245/researchers-find-smart-meters-could-reveal-favorite-tv-shows/, accessed 27 April 2013; Greveler, U., Justus, B., Loehr, D. (2011) Multimedia Content Identification Through Smart Meter Power Usage Profiles, available online at: http://epic.org/privacy/smartgrid/smart_meter.pdf, accessed 27 April 2013

[588] Enev, M., Gupta, S., Kohno, T., Patel, S. (2011) Televisions, video privacy, and powerline electromagnetic interference, *Proceedings of the 18th ACM Conference on computers and communications security*, pp. 537-550

[589] See Smart Grid Coordination Group (2014) Document for the M/490 Mandate Smart Grid Information society, available online at: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf (last accessed: 29.4.2015), p. 80

[590] Wynn, G. (2010) Privacy concerns challenge smart grid rollout, Reuters 25 June 2010, available online at: http://www.reuters.com/article/2010/06/25/energy-smart-idUSLDE65N2CI20100625 (last accessed: 13.5.2015), cites Martin Pollock of Siemens Energy stating: "*We, Siemens, have the technology to record it (energy consumption) every minute, second, microsecond, more or less live…. From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data*."

data protection is recognized also in the Member States as it is the case of the Privacy Impact Assessment on smart metering done in the UK. With regards to this assessment, for privacy reasons and also in compliance with the proportionality principle suppliers of energy are allowed to access the data on daily frequency and not with the half-hourly intervals, with the exception of the cases in which they receive explicit consent from the customer.[591] The daily access of the suppliers to the data does not mean, however, that the system is also collecting the data at such an interval. This is also because for the consumers to benefit from the system there is the need to have a more frequent access to their energy consumption data. Law enforcement authorities have therefore the possibility to access the generated data frequently, either directly or via third parties.

Mass surveillance might be yet another possibility for the use of smart meter data from law enforcement authorities. This might be the case when the authorities will target an illegal activity (for example cultivation of narcotic plants) and check all smart meter data from households for identifying cases of law infringement.

4.2.4 Challenges that surveillance with smart meters presents to the right to privacy

Surveillance is by definition the way in which the State interferes with the private sphere of individuals. However, this interference is not automatically unlawful as long as it is balanced against other interests of the society and the citizens.[592] When deciding on State surveillance with smart meters it has to be kept in mind the level of intrusion into the private sphere of the citizens of this device that has a 24 hours presence within a household. The all-continuous and uninterrupted presence of the devices has the result that also the challenges created to the right to privacy will be more severe. That is the reason why the need for a warrant similar with the one needed for searching a home has been advised, when smart meter data is to be obtained for surveillance purposes.[593] This suggestion is not surprising, given that in European law as well as in most constitutional systems of the Member States, the inviolability of the home is regulated now within the realm of the protection of the right to privacy (despite the fact that the right to have the home protected was historically recognized earlier in the constitutional systems than the right to privacy).[594]

As already stated above, smart meter data can be of interest for law enforcement authorities, therefore the potential to use them for surveillance cannot be neglected. Surveillance via smart

[591] Recital 2.10, UK Smart metering implementation programme PIA 2012, available online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43044/7226-sm-privacy-ia.pdf (last accessed: 4.1.2016)

[592] Himma, K.E. (2007), Privacy vs. Security: Why privacy is not an absolute value or right, San Diego Law Review, vol. 45, 2007, pp. 859-922

[593] EDPS (2012) Opinion of the European Data Protection Supervisor on the Commission Recommendation on preparations for the roll-out of smart metering systems, para. 50

[594] De Hert, P., Koops, B.-J., Leens, R. (2009) Constitutional rights and new technology: A comparative perspective, in Pawels, C. et al (eds), *Rethinking European media and communications policy*, pp. 319-350

meter data can be performed by law enforcement authorities that access the data directly or via service providers and other parties, or can be performed by service providers in those cases in which they are under a duty to refer suspicious cases and therefore operate as an arm of the State.[595] In situations in which service providers collaborate with public authorities for surveillance purposes the States are asked[596] to take the necessary steps to protect individuals against abuses of human rights by these entities in accordance with UN Resolution 17/4[597] and the Guiding principles on business and human rights.[598] As of May 2018, the EU legislation that applies to law enforcement authorities (Directive 2016/680) will apply also to third parties that collect and process personal data for the scope of law enforcement.

The aim of this section is to assess the challenges that surveillance via non-purpose built technology creates to the right to privacy in the concrete study case of smart meters. In chapter 2 these challenges were identified as: (1) the increased risk for incidental surveillance, (2) facility of engaging in mass surveillance, and (3) possibility for retroactive surveillance. Each of these challenges is discussed below in a separate subsection.

4.2.4.1 Incidental surveillance

Incidental surveillance was seen in chapter 2 as the accidental collection of data on individuals that are not the target of the surveillance activity[599] with the effect of interfering with their private life. It was already argued that thus far, there is no proper protection of the privacy of individuals that find themselves in situations of incidental surveillance in the European Union. The legislation does not regulate such situations while in the case law of the European Court of Human Rights this form of surveillance is considered as being compatible with article 8 ECHR, even though the standards set in the article are not assessed in situations of incidental surveillance.[600]

---

[595] In general on the qualification of private entities as emanations of the State for specific purposes see: Chalmers, D., Davies, G., Monti, G. (2014) European Union Law, 3rd edition, Cambridge, p. 312; case C-180/04 Vassallo v. Azienda Ospedaliera Ospedale San Martino di Genova e Cliniche Universitarie Convenzionate [2006] ECR I-7251, para. 26. For situations in which surveillance performed by individuals has qualified as State surveillance see: M.M. v. The Netherlands, ECHR application no. 39339/98, 8 April 2003, para. 42; A. v. France, ECHR application no. 14838/89, 23 November 1993, para. 38-39

[596] See Resolution 2045(2015) of the Parliamentary Assembly of the Council of Europe on Mass Surveillance, 21.04.2014, para. 6

[597] See Resolution 17/4 adopted by the Human Rights Council on Human rights and transnational corporations and other business enterprises, 6.7.2011

[598] See Guiding principles on business and human rights – Implementing the United Nations "Protect, Respect and Remedy" framework, annexed to the Human Rights Council Report (A/HRC/17/31) and endorsed in Resolution 17/4, para. 4

[599] In a guiding document to the UK Regulation of Investigatory Powers Acts 2000, the Leeds City Council Legal Services refer to what is defined for this study as "incidental surveillance" as "collateral intrusion", or "*interference with the privacy of persons, other than the subject of the surveillance*", available online at: http://www.leeds.gov.uk/docs/RIPA%20Guidance%20and%20Procedure%20-%20May%202013.pdf (last accessed: 30.03.2015)

[600] Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 28

Surveillance via smart meters involves incidental surveillance of all the members of a household and even of temporary guests. In the way, smart meters operate, they communicate data on the energy consumption of an household and not of single individuals. The attribution of data to individuals comes as the result of profiling and analysing. This implies the analyses of all the transferred data from all the relevant individuals, and therefore an open possibility for incidental surveillance.

Essentially two possibilities for an *ex post* protection of his rights exist for an incidentally surveilled individual. The first possibility is to challenge the validity of the surveillance mandate as if it was directed to him, and the second consists in asking the deletion of the incidentally collected data.

The first possibility applies when the incidentally surveilled individual faces as a result of the information gathered a case before a court. A similar situation was discussed in *Lambert* where the European Court of Human Rights focused on the existence of legal safeguards and made 'effective remedy' available for incidentally surveilled individuals.[601] In this case the ECtHR gives the incidentally surveilled individuals the possibility to challenge the validity of the surveillance mandate as if they were in person addressed by it.[602] The possibility for 'effective remedy' is an *ex post* adjustment and improves only partially the situation of the incidentally surveilled person. In issuing the surveillance mandate the authorities have not been considering the necessity and proportionality of the State interference in the concrete situation of the incidentally involved individual and therefore it would be difficult to successfully challenge the mandate on its merits.

The second possibility is to delete the data once these do not have any more relevance for the investigation or in alternative to notify the concerned individual, as stated in Recommendation R87(15) of the Council of Europe to the Member States.[603] Such *ex post* notification has a specific importance for the protection of individuals in cases of incidental recording of data since it is an essential safeguard against abuse of monitoring powers and it is an important part of the right to an 'effective remedy' before the national courts. This important Recommendation does not have, however, any binding effect, and has not been incorporated so far in the national legislation of most of the Member States.[604] The European Court of Human Rights has applied the 'notification' principle

[601] Lambert v. France, ECHR application no. 23618/94, 24 August 1998, para. 40
[602] Lambert v. France, ECHR application no. 23618/94, 24 August 1998, para. 38
[603] Recommendation R87(15) of the Council of Europe, principle 2.2. In general, on the problems following the non-binding nature of R87(15) see Study on Recommendation No. R(87)15 of 17 September 1989 regulating the use of personal data in the police sector – 'Data Protection Vision 2020: Options for improving European policy and legislation during 2010-2020' by Joseph A. Cannataci, available online at: http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf (last accessed: 20.2.2015); Cannataci, J., Caruana, M. (2013) Report: Recommendation R(87)15 Twenty-five years down the line, available online at: http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf (last accessed: 20.2.2015)
[604] De Hert, P., Boehm, F. (2012) The rights of notification after surveillance is over: Ready for recognition?, in Bus et al. (eds.), *Digital enlightment year book 2012*, IOS Press, p. 19

in a number of cases.[605] The most significant decision is *Ekimdzhiev* were the ECtHR clearly established that omission of notification of surveillance measures, once it does not risk to jeopardize the inquiry, amounts in itself to a violation of article 8 ECHR.[606] The use of *ex post* notification of surveillance measures has special importance for the individuals in cases of incidental surveillance since there is no other possibility to know and challenge this surveillance in case they would not arrive before the national courts. For these cases, *ex post* notification would serve as an essential safeguard against abuse of monitoring powers and as an important part of the right to an 'effective remedy'.

From the examples above it is clear that the right to privacy of individuals that find themselves in situations of incidental surveillance is not properly protected. This important conclusion has to be taken into account when deciding on the use of surveillance via smart meter data that per definition effects all the members (and temporary guests) of a household and therefore also untargeted subjects of surveillance.

Another element, related with profiling and analysing the data as well as with the possibility of incidental involvement of individuals in surveillance is the accuracy of the data. As already seen, smart meters refer the energy consumption and activities of a household and not of single individuals. Processing of data and linking them with other sources gives the possibility to single out and distinguish the activities of different individuals, but there is always a possibility for errors which cannot be ignored.[607] This might be the case in situations in which one member of the household engages in an activity that is always attributed to another member (e.g. 9 years old daughter watches a football match while the father is not at home). This possibility should be taken into account when deciding on the employment of these data for surveillance.

The new Data Protection Directive does not address situations of incidental surveillance. Even though it introduces a right to information on the individuals whose personal data are processed for the purpose of prevention, detection, investigation and prosecution of crime, this is done on the basis of a request from the data subject.[608] Since, if not informed, it is difficult for a data subject to know that their data have been incidentally collected, the exercise of the right to information is most likely not going to be effective.

[605] Klass v. Germany, ECHR application no. 5029/71, 6 September 1978, para. 50; Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 114

[606] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, ECHR application no. 62540/00, 28 June 2007, para. 91

[607] Beckel, C., Sadamori, L., Staake, T., Santini, S. (2014) Revealing household characteristics from smart meter data, *Energy*, vol. 78, pp. 397-410

[608] Directive 2016/680, arts. 12-14

4.2.4.2 Mass surveillance

In chapter 2 it was seen that there is evidence that mass surveillance programmes are used extensively in some Member States of the EU[609] and they enable intelligence services and law enforcement authorities to access, without an individual warrant personal data on a large scale. Mass surveillance is considered as a pre-emptive measure with the aim to identify and avert serious dangers, such as an armed attack or terrorist attack, which threatens the national security of a country as well as other criminal activities disturbing the public security.[610] The interest of law enforcement authorities for smart meter data as well as the large-scale availability of these data gives the possibility to use the devices in large mass surveillance programmes.

The remedies that individuals have in cases of mass surveillance are quite limited. This is linked also with the fact that most of the time individuals are not aware that they have been the subject of such measures. In this framework, the European Court of Human Rights extended the application of article 8 ECHR and of the test it has established for cases of individual surveillance also to cases of mass surveillance. For the Court there are no grounds to apply different principles concerning the accessibility and clarity of the rules governing individual surveillance, on the one hand, and more general programs of surveillance, on the other.[611] The 'effective remedy' that individuals have in such situations is the possibility to challenge the mass surveillance programs as such, without the need to prove that they have been individually subjects of them since otherwise article 8 ECHR "*would be reduced to a nullity*".[612]

Apart special mass surveillance programmes that are operational in different Member States, the EU with the (now invalidated)[613] Data Retention Directive[614] was considered as introducing a form of

[609] Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf> accessed 1 November 2013; see also the Explanatory memorandum on the Parliamentary Assembly of the Council of Europe draft Resolution and draft Report on Mass Surveillance prepared by Mr. Pieter Omtzigt, rapporteur, available online at: http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21583&lang=en (last accessed: 28.4.2015), para. 26-29

[610] Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 4; In a resolution of the Parliamentary Assembly of the Council of Europe it was stated, however, that in the United Stated independent reviews have shown that mass surveillance has not contributed to the prevention of terrorist attacks thus far. "*Instead, resources that might prevent attacks are diverted to mass surveillance, leaving potentially dangerous persons free to act.*", see Resolution 2045(2015) of the Parliamentary Assembly of the Council of Europe on Mass Surveillance, 21.04.2015, para. 11

[611] Liberty and Others v. The United Kingdom, ECHR application no. 58243/00, 1 July 2008, para. 63

[612] Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 78; Association "21 December 1989"and Others v. Romania, ECHR applications 33810/07 and 18817/08, 24 May 2011, para. 167

[613] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238

[614] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006

mass surveillance at Union level.[615] The Directive essentially required the retention of metadata from electronic communications for periods of time between six months and 2 years.[616] This was based on the ability of service providers to collect and retain a number of personal data for different purposes (as for example billing details) and then use these data for other purposes, in the concrete case the data was used for mass surveillance of the users of electronic communications.

There is an essential difference between the way the retention of data was done on the basis of the Data Retention Directive and other databases created at European level, as for example EURODAC,[617] SIS II[618] or VIS.[619] These databases were created with the aim to collect and retain personal data while the Data Retention Directive aimed to benefit from the way of operation of electronic communications and suggested to change the purpose of the data collected for service purposes and use them for law enforcement ones. Advancement in technology makes it easier in the future to use the same scheme as under the Data Retention Directive for the massive accessing of personal data collected for other purposes.

Even if there is not yet any evidence of the employment of smart meter data for mass surveillance purposes, this might be a possibility. In the invalidation of the Data Retention Directive the European Court of Justice found data retention in the concrete case to be an appropriate method for attaining the objective of fighting serious crime, but specified that it needed to be proportionate. The use of retained data for surveillance challenges, however, the right to privacy.

As already stated and argued in the literature, analyses of smart meter data reveals details on the life and activities taking place within a household similar to situations in which there is a physical presence of the investigator on the premises. That is also the reason why the EDPS recommends mandates similar to the ones needed to enter one's private premises in the cases of accessing smart meter data for surveillance purposes. This recommendation would exclude per definition the use of smart meter data for mass surveillance since it will require a specific mandate each time data are accessed.[620] A routine control of retained smart meter data is tantamount to a routine control inside

[615] Roberts, H., Palfrey, J. (2010) The EU Data Retention Directive in an era of internet surveillance, in Deibert, R. et al. (eds.) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT, pp. 35 - 53
[616] Art. 6 Directive 2006/24/EC
[617] Council Regulation (EC) no 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15/12/2000
[618] Regulation (EC) no 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006
[619] Regulation (EC) no 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008
[620] Also PACE rapporteur Omtzigt suggests that mass surveillance practices in general must be substituted with data collection after consent or court order granted on the basis of reasonable suspicion. See Explanatory memorandum on the Parliamentary Assembly of the Council of Europe draft Resolution and draft Report on Mass Surveillance prepared by Mr. Pieter Omtzigt, rapporteur, available online at:

houses and this goes against the right to privacy and the inviolability of the home. That is why we argue and advice against such controls for detecting potential illegal activities taking place within a household. The level of intrusiveness of this method of surveillance is to be taken into account when deciding on mass surveillance of smart meter data.

4.2.4.3 Retroactive surveillance

The possibility that non-purpose built devices create for retroactive surveillance, was seen in chapter 2 as interfering with the right to privacy as well as with the safeguards and the effectiveness of a legal process.[621] Even though there is not yet any legislation requiring smart meter data retention for law enforcement purposes, service providers or other parties that have access to the data might keep data for long periods of time for other reasons than surveillance. The Measuring Instruments Directive, for example, in Annex MI-003, para. 5(3) establishes that smart meter data shall remain available for reading for a period of at least 4 months. This period of retention might change from Member State to Member State in relation with the electricity payment intervals. In UK for example the customer is sent a bill every 1 to 3 months, but this might be an estimate bill while an accurate bill is sent every 2 years. Smart meter data would then be retained in UK for at least 2 years for billing purposes. In Poland on the other side, the system is similar but the invoice is issued every 6 months.[622]

Smart meter data, even if not detailed, may be retained also for other purposes than billing needs. An example are taxation purposes which require the retention of the data for (e.g.) 3 years in the UK, 5 years in Poland, 7 years in the Netherlands, 10 years in France.[623] In addition, for insuring the benefits that smart meters are said to provide to service providers and the electricity companies, one might expect that they would retain the metering data themselves for an accurate forecasting of energy needs and the designing of their future purchasing strategies.

The retention of the data, independent from the purpose, gives the possibility to law enforcement authorities to access them and surveil as a result past activities and trends of behaviour of the individuals that present an interest for them. The retained data create the possibility to scrutinize the past, in a time in which the individual was not under suspicion and no mandate for his surveillance was issued, and bring it to the present. Unfortunately, the enlarged possibilities for law enforcement authorities to access available data bring with them also a lack of transparency on the quantity and

---

http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21583&lang=en (last accessed: 28.4.2015), para. 113

[621] Milaj, J., Mifsud Bonnici, J.P. (2014) Unwitting subjects of surveillance and the presumption of innocence, *Computer Law & Security Review*, vol. 30, no. 4, pp. 419-428

[622] See Essential regulatory requirements and recommendations for data handeling, data safety, and consumer protection, Recommendation to the European Commission, 5 December 2011, para. 100

[623] Essential regulatory requirements and recommendations for data handling, data safety, and consumer protection, Recommendation to the European Commission, 5 December 2011, para. 105

quality of the data accessed and analysed. This might be the situation in both individual surveillance cases as well as in mass surveillance cases.

For cases of individual surveillance via smart meters one might argue that the period of time in which surveillance will take place will be clearly defined in the surveillance mandate which might limit surveillance to present and (potentially) future activities. On the other side, for being able to link the data to specific individuals and have the real fruits of the surveillance activity, an analysis of historical data is required. Therefore, the possibility for retroactive surveillance is present and not negligible.

Mass surveillance on the other side is done per definition in the absence of a specific surveillance mandate and of a specific suspicion. As a result, the private sphere of the individuals is scrutinized in these cases at the time there is not any indication for their involvement in a criminal activity.

Retroactive surveillance via smart meter data is easily performed due to the advanced technology but, apart problems to the right to privacy it creates problems also for the right to presumption of innocence as a legal safeguard for the individual during a criminal procedure and compromises therefore the effectiveness of the legal process**.** The problems created for the rights of the individuals must be taken into account by the national authorities issuing a surveillance mandate.

4.2.5 Concluding remarks

Law enforcement authorities might be quite tempted to use smart meters and the data they collect for surveillance. Smart meters are, therefore, a clear example of devices that are not designed nor introduced for surveillance purposes but that might be used as such. The use of smart meters for surveillance might be the result not only of the amount and detail of the collected data and of the easiness in accessing them but also of economic conveniences. With regards to the latest one must bear in mind that smart meters are installed in the European households as part of a general European energy saving project and collection and communication of data is a feature of these devices without requiring any investment from law enforcement authorities. Also retention of data, even if not yet required by the laws for law enforcement purposes, is already present in the system for other purposes than surveillance and for relatively long periods of time. Economic and technical conveniences should, however, not turn to a burden for individuals and their protection of fundamental rights.

The assessment of smart meters as an example of non-purpose built devices that have a potential to be used for surveillance gave the possibility to concretely analyse the effects of this form of surveillance for the right to privacy of the individuals. It was seen in this section that in case these devices are used for surveillance purposes, sufficient safeguards for protecting the right to privacy are missing and as a result individuals are exposed to potential infringements of their rights.

Surveillance via smart meters is prone to present all the challenges to the right to privacy that were identified as problematic for surveillance with non-purpose built technology in general in chapter 2 of this study (i.e. situations of incidental surveillance, mass surveillance and retroactive surveillance). It was argued that this form of surveillance presents the clear danger to expose individuals to such situations for which the protection of their rights is not adequately guaranteed.

The level of interference of smart meters with the life of individuals was evaluated as very intrusive. It effects different aspects of the right to privacy as the inviolability of the home, of the private life and of the family life. This is the result of the presence and operation of these devices continuously for 24 hours within a household that is compared with a 24 hours presence of a physical surveillant within the premises. The need for surveillance warrants similar with the ones for searching private premises was therefore supported in cases of accessing smart meter data for law enforcement purposes, which would imply on the other side not to make use of these devices in the framework of mass surveillance programmes.

Even though surveillance is mainly a national activity regulated by the realm of national laws, the protection of fundamental rights of the individuals falls within the scope of application of European rules. National authorities have therefore to comply with the European standards when authorizing and using smart meters for the purpose of surveillance and harmonized European rules are desirable for regulating surveillance with these devices. Thus far, the specific legislation on smart meters does not regulate situations in which the privacy or personal data of individuals are interfered with. In such a situation one must turn to the general rules while waiting for more specific ones to be adopted. Keeping in mind the high level of intrusiveness with the privacy of the individuals as well as the challenges created for the right to privacy and the current incomplete set of safeguards, it is important for the national authorities to carefully assess the necessity and the proportionality of the use of smart meters for surveillance purposes.

4.3 Smart phones

This section addresses the use of smart phones for surveillance purposes, though it has to be kept in mind that one section is not enough for considering all the possible uses of smartphones for surveillance purposes. The section does not have neither the ambition nor the aim of being exhaustive. In light of the theoretical findings of the previous chapters, the section challenges itself to contribute to the existing literature by focusing on the problems that surveillance via smartphones, as non-purpose built surveillance devices, creates for safeguarding the right to privacy of European citizens in the current European legal framework. Attention is paid to the different surveillance properties of the device. Since the interception of communications is already largely considered in the case law of the ECHR and also in different parts of this research, the section will

focus mainly on surveillance and dataveillance via the heterogeneous types of data that smartphones host such as: messaging data, usage history, application data, sensor data, user input data, etc.[624]

In sub-section 4.3.1 is presented some background information on smartphones in general and on the type of data that can be accessed via them. In sub-section 4.3.2 are discussed the possibilities of law enforcement authorities to use smartphones for surveillance purposes. In sub-section 4.3.3 are discussed the challenges that the use of smartphones for surveillance creates to the right of the individuals to a protected private life. The conclusions are presented in sub-section 4.3.4.

4.3.1 Background information on smartphones

Smartphones are great technology inventions that have increased in popularity due to their limited dimensions, their capabilities, as well as the easy access and use which make them perfect for use as portable computer devices.[625] Theoharidou et al. (2012) define smartphones as "*…a cell phone with advanced capabilities, which executes an identifiable operating system allowing users to extend its functionality with third party applications that are available from an application repository.*"[626] Smartphones can thus be defined as mobile phones with computing capabilities, typically offering internet access, e-mail capability, data storage, music and movie player, camera and camcorder, GPS navigation, a virtual assistant with voice recognition, etc. Their assets include private information (contacts, communication metadata, location information, etc.), device resources (CPU, RAM, battery, etc.) and applications (apps).[627]

Smartphones enable advanced interactions between individuals through thousands of available applications.[628] Real-time social networking, for example, creates possibilities not only for exchanging ideas or even discussing work related issues, but also for sharing information to discover nearby friends (using for example Google Latitude). Many of the existing applications are able to perfect their services context based. For doing this they rely on relevant data that are available via the smartphone and generated by the smartphone users themselves with regards to their environment and behaviour or even generated by sensors.[629] The collection of such data is closely linked to the

[624] See Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., Gritzalis, D. (2012) Smartphone forensics: A proactive investigation scheme for evidence acquisition, in Gritzalis, D. et al. (eds.), *Information security and privacy research*, pp. 249-260

[625] Jung, Y. (2014) What a smartphone is to me: Understanding user values in using smartphones, *Information Systems Journal,* vol. 24, no. 4, pp. 299-321

[626] Theoharidou, M., Mylonas, A., Gritzalis, D. (2012) A risk assessment method for smartphones, in Gritzlis, D. et al. (eds.) *Information security and privacy research*, pp. 443-456

[627] Jeoen, W., Kim, J., Lee, Y., Won, D. (2011) A practical analyses of smartphone security, in Smith, M.J., Salvendy, G. (eds.) *Human interface*, pp. 311-320

[628] Article 29 Working Party (2011) Opinion 13/2011 On geolocation services on smart mobile devices, 16 May 2011

[629] Lane, N.D. et al. (2010) A survey of mobile phone sensing, IEEE Communications Magazine, vol. 48, no. 9, pp. 140-150; Apart the apps that are software, smartphones are furnished also with hardware such as cameras, microphones, etc. that operate as sensors and may collect as well personal data

fact that smartphones are typically with their users on a 24 hours basis and therefore a good means for collecting tons of relevant personal data and information. Some of the collected personal data can be: contacts, addresses, locations, financial information, etc.

The use of smartphones is not only limited to communications. Nowadays, individuals often use them to perform tasks that were once exclusively performed on PCs. This increases the amount and the type of data that are collected and accessible via smartphones. Among these data, the ones that qualify as personal are particularly relevant for this study. As long as they are linked to an identified or identifiable person they fall under the EU data protection and privacy rules.

Privacy concerns linked with the use of smartphones have accompanied their proliferation. For example, with regards to the many available apps,[630] it is often complained that currently the operating system of smartphones fails to provide users with information on the data that they collect and share with third parties.[631] There is a lack of transparency on the data collected from applications, the legality of such a process as well as on the consent (informed or not) given by the users. Apps are designed for facilitating various extra uses of the device, as for example to access quick information on the news, weather, gaming, social networks, online shopping, banking, etc.[632] The uncontrolled access and collection of personal data makes users and their personal data quite vulnerable in such a context.[633]

Apps are especially active in collecting and transferring personal data as well as in tracing users and the later are not always aware of all their activity.[634] It is therefore quite surprising to find out that smartphone users appear not to worry about privacy and security risks in the use of applications. A survey done in 2012 shows that the majority of smartphone users believe that downloading apps from the apps repository is risk-free and only 3,5% of the interviewed consider privacy and security when deciding to download an app.[635] According to the data available from Gartner, a marketing

[630] It has been reported that more than 1600 new apps are added to app stores daily

[631] Enck, W. et al. (2014) TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones, *ACM Transactions on Computer Systems*, vol. 32, no. 2, pp. 29; Sipior, J.C., Ward, B.T., Volonino, L. (2014) Privacy Concerns Associated with Smartphone Use, *Journal of Internet Commerce*, vol. 13, no. 3-4, pp. 177-193

[632] Zallone, R. (2014) Here, there and everywhere: Mobility data in the EU (Help needed: Where is privacy?), *Santa Clara High Tech. L.J.*, vol. 30, no. 1, pp. 57-88; OECD (2014) Measuring the digital economy: A new perspective, pp. 30-31

[633] Gomez-Martin, L.E. (2012) Smartphone usage and the need for consumer privacy laws, Pittsburgh Journal of Technology Law, vol. 12, no. 2, pp. 1-21; Martinez-Perez, B., Torre-Diez, I., Lopez-Coronado, D. (2014) Privacy and security in mobile health apps: A review and recommendations, *Journal of Medicine Systems*, vol. 39, no. 181, doi:10.1007/s10916-014-0181-3

[634] ENISA (2015) Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics; Article 29 Working Party (2013) Opinion 2/2013 On apps on smart devices, 27 February 2013

[635] Mylonas, A., Kastania, A., Gritzalis, D. (2013) Delegate the smartphone user? Security awareness in smartphone platforms, in *Computers and Security*, vol. 34, pp. 47-66

research company, in 2012 were downloaded 57,3 billion free and 6,65 billion paid apps.[636] The trust that smartphone users have in the technologies they possess might come from an under evaluation of the fact that smartphones are a combination of feature phones and computers and therefore they are endangered from risks that might attack singularly each of these devices.

In guidelines prepared by the EDPS on the protection of personal data in mobile devices used by the European institutions are listed the most relevant risks to personal data collected or stored in mobile devices.[637] These identified risks are:

a) accidental loss of personal data;
b) an alteration or destruction of personal data due to an unlawful access to users' personal data by mobile device administrators, including remote switch off and remote alteration/wiping of personal data (photos, videos, local contacts, local copies of e-mails, documents, etc.);
c) leakage of personal data due to non-authorized access to those data possibly also causing reputational or financial damages to the EU institutions;
d) unlawful geographical location of the user by potential attackers via location services;
e) identity theft through the compromise of credentials (usernames, passwords, certificates) stored on mobile devices.

Closely linked to the risks one might identify the threats that could lead to them. These identified threats for the EDPS are:

a) the unlawful collection and processing of personal data by applications or devices themselves;
b) customisation by device manifacturers, carriers and OS developers leading to locked configurations and features;
c) a hackers attack;
d) accidental lost or theft of the device;
e) physical installation/modification of applications;
f) a misuse or human error of the user that disables security firewalls or ignores security warnings.

Even though in the EDPS guidelines the risks and threats are presented as relevant for the protection of the EU institutions in those cases in which a mobile device is used for work related purposes, they are relevant also for individual's personal data independent from any institutional affiliation. Furthermore, from the above identified risks and threats a conclusion can be drawn regarding the use of smartphones for surveillance purposes. Despite smartphones being a goldmine of data they present risks and threats and are vulnerable to external interventions which might make the

[636] See statistics online at: http://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/ (last accessed: 23.2.2016)
[637] EDPS (2015) Guidelines on the protection of personal data in mobile devices used by the European Institutions, available online at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/15-12-17_Mobile_devices_EN.pdf (last accessed: 27.1.2016), p. 23

accessed data not completely reliable in all situations. In the following section, we will discuss the relevance of smartphones for surveillance purposes.

4.3.2 Smartphones relevance for law enforcement authorities

Smartphones create lots of opportunities for performing different forms of surveillance. They merge with a person's everyday life and are characterized by the diversity of the data collected. The smartness of the device creates the possibility to be used for direct surveillance, as in the case of interception of communications, as well as for dataveillance. The combination of the proprieties of a phone with the computer capabilities gives rise to enormous possibilities for data collection. These data can be content related, metadata, data stored in the device as, for example, contacts, photos and videos, present or past locations and even user's behaviour and interests (through internet search terms, for example) and sometimes even passwords, financial data or credit card numbers. Smartphones can be used also indirectly for surveillance in those cases that users become active as surveillants and collaborate in law enforcement activities. This sub-section discusses first the use of smartphones by law enforcement authorities and then crowd-sourced policing.

4.3.2.1 Smartphones used for surveillance by law enforcement authorities

There are different ways in which data are generated in smartphones. Mylonas (2013)[638] categorises the data sources of a smartphone as: messaging data, device data, sim card data, usage history data, application data, sensor data and user input data. Smartphones are, for example, furnished with hardware, as for example: microphone, camera, location sensors (i.e. GPS), motion sensors (i.e. accelerometer), and environmental sensors (e.g. light, temperature, pressure), etc. As a result of these inbuilt hardware a number of personal data are generated as for example pictures, videos, data on locations or itineraries, etc.[639] Sensors provide data that can help to create context awareness (for example, if a user is in a bright or dark environment) and can help to build hypothesis or to verify an alibi. Sensors can be used for direct surveillance, as in the case of location tracing, or for dataveillance. One has to keep in mind, however that not all sensor data can be collected retroactively (for example one cannot retroactively infer keystrokes from a nearby keyboard via the smartphone accelerometer).[640] Beside sensors which are pre-installed in a device, there is the possibility to install third-party software, as in the case of applications. Applications are also said to be quite active in collecting personal data and even accessing different functions of the device for collecting these data.

[638] Mylonas, A. (2013) Security and privacy in ubiquitous computing: The smart mobile equipment case, *Technical report series (Athens University)*, no. 3, pp. 139-141

[639] Landau, S. (2015) Control use of Data to Protect Privacy, *Science*, Vol. 347, no. 6221, DOI: 10.1126/science.aaa4961

[640] Marquardt P., Verma A., Carter H., Traynor P. (2011) (Sp)iphone: decoding vibrations from nearby keyboards using mobile phone accelerometers, in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, pp. 551–562

The data generation in smartphones is, therefore, strongly linked with the design and capabilities of the device and its operating system. These are, however, not the only ways data are generated in smartphones. Individual users furnish their devices with large quantities of personal data. They actively store personal data on the device as for example contacts, agendas, etc. or even generate and store new data as for example when shooting pictures, videos, etc.

The different data sources can furnish relevant information to be used by law enforcement authorities or as evidence at a court case. Mylonas (2013)[641] presents this relevant information on the basis of a taxonomy of evidence types identified by Zahman (1987).[642] Law enforcement can be interested in messaging data, for example. These data can reveal apart the content also metadata that identify the subject and the time of communication. Device data (e.g. the IMEI code of the device) can be used to determine a subject from the providers' records. In the same fashion, also SIM card data can be used to identify a device owner. Usage history data can serve for determining the time of an event or can be used to determine the device location. Application data may serve to determine locations, to identify individuals, and to access other data stored in the device. Sensor data can be used to infer the devices' context. For instance, a microphone can be remotely enabled and collect speech data.[643] Also with regards to location evidences, the correlation is strong due to the popularity and location accuracy of GPS sensors. Apart other uses, user input data can serve to uniquely identify a subject via keystroke analysis.[644]

The design and function of smartphones allows law enforcement authorities to collect data in real-time or to aim retroactively for historic data. The data (or parts of them) can be collected directly from the device itself. Law enforcement may also collect the data from other sources as for example from the service providers, or even from third parties applications (even though this last possibility has to be used with care since the collection of personal data from applications might be in certain situations unlawful and not in conformity with the rules on the free and informed consent from the users and therefore cause an even bigger problem to the protection of their rights to privacy and data protection). It is not a surprise therefore that the use of smartphones for surveillance purposes is becoming even more attractive for law enforcement authorities.

[641] Mylonas, A. (2013) Security and privacy in ubiquitous computing: The smart mobile equipment case, *Technical report series (Athens University)*, no. 3, pp. 139-141

[642] Zachman J. (1987) A framework for information systems architecture, *IBM Systems Journal*, vol. 26, no. 3, pp. 276–292

[643] McCormack, D. (2013) Ex-FBI official claims organization can remotely activate the mic on Android phones to record user's conversations, in *Daily Mail*, 2 August 2013, available online at: http://www.dailymail.co.uk/news/article-2383892/Ex-FBI-official-claims-organization-remotely-activate-mic-Android-phones-record-users-conversations.html (last accessed: 12.2.2016)

[644] Moskovitch, R., et al. (2009) Identity theft, computers and behavioral biometrics, in *Proceedings of the IEEE International Conference on Intelligence and Security Informatics,* pp. 155–160

Collection of smartphone data certainly requires some technical skills and logistics.[645] The big possibilities for data collection that the devices offer have already instigated the creation of tools which perform either physical (one by one) or logical (grouped) collection of data in different systems, as for example: Windows Mobile,[646] Symbian,[647] iOS[648] and Android.[649]

The examples above showed that smartphones are a valuable source of data and means of surveillance for law enforcement authorities. They create the possibility for different forms of surveillance, and access to heterogeneous data which might be relevant also for the validation of alibis or the building of hypothesis. These data can be accessed either directly from the device or through other parties.

4.3.2.2 Crowd-sourced policing

The capabilities of smartphones and their popularity have influenced also the creation of a new form of surveillance, the so called crowd-sourced policing.[650] In this emerging new form of surveillance, law enforcement authorities rely on the collaboration and input of individuals that find themselves at certain locations at relevant points in time without the need to have any direct access on their devices.[651] Said differently, in crowd-sourced policing the State surveills through the eyes of its fellow citizens. Development of technology has thus created the possibility not only for non-purpose built devices to be used for surveillance but also for non-specialized individuals to become surveillants.

Used in Europe as well, one of the most prominent examples of such form of surveillance method comes from Canada. During the Vancouver riots in 2011 many people used their smartphones to make pictures of the participants and to document the social event. Social media (a Facebook page dedicated to the riots) was then used for sharing the data.[652] This gave the possibility to the police to

[645] Bennett D. (2012) The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations, in *Information Security Journal: A Global Perspective*, vol. 21, no. 3, pp. 159-168

[646] Casey E, Bann M, Doyle J. (2010) Introduction to windows mobile forensics, *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, vol. 6, no. 3-4, pp. 136-46

[647] Distefano A., Me G. (2008) An overall assessment of mobile internal acquisition tool, *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, vol. 5 (supplement), pp. 121-127

[648] Husain M.I., Sridhar R. (2010) iForensics: Forensic analysis of instant messaging on smart phones, in Goel S. et al. (eds.) *Digital Forensics and Cyber Crime*, Springer, pp. 9-18

[649] Thing V.L., Ng K.Y., Chang E.C. (2010) Live memory forensics of mobile phones, *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, vol. 7, (supplement), pp. 74–82

[650] Crowd sourced surveillance is different from open-source intelligence that is based on publicly available sources and which is not discussed in this chapter since smartphones are only one of the devices for publishing or accessing data in social-networking sites, video sharing sites, etc. The author though submits that the use of smartphones might increase the possibilities and the input for this form of intelligence

[651] Marx, G. (2013) The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes, *Security and Privacy, IEEE*, vol. 11, no. 5, pp. 56-61; Reeves, J. (2012) If you see something, say something: Lateral surveillance and the uses of responsibility, in *Surveillance and Society*, vol. 10, no. 3, pp. 235-248

[652] Schneider, C.J., Trottier, D. (2012) The 2011 Vancouver riot and the role of Facebook in crowd-sourced policing, in *BC Studies*, no. 175, pp. 57-72

identify many rioters with pictures and names on the bases of comments of other social media users even as the riot continued. In another occasion, during the Boston bombing in April 2013, online forums such as Reditt started independent efforts to identify the bombers based on input from commenters. This activation of citizens was before the FBI had singled out any images of potential suspects.[653]

Crowd-sourced policing has also its drawbacks. The active self-involvement of non-specialized individuals in surveillance might at times be damaging for the police and intelligence actions as well as lead to incorrect information[654] or even agitate people during mass disorders.[655] As an example it can be mentioned the search for suspects in Brussels, in the aftermath of the Paris attacks in November 2015, when the police had to ask the users of Twitter for blackout since too much activism was revealing the police moves to the world in real time.[656] This new form of surveillance might also bring in specific cases perverse incentives to erroneously identify and publicize information on individuals that turn out not to be suspects.[657]

Crowd-sourced policing can be instigated by the law enforcement authorities or in other cases can be based on the initiative and will of the citizens themselves that want to contribute to the public security. In the first situation when the citizens are asked to act as the arm and the eye of the State there is no doubt that the situation falls under the protection of the right to privacy and Article 8 ECHR.[658] In those other cases in which the individuals act out of their own initiative we argue that the European data protection rules[659] still apply.

In *Rynes* with regards to a private CCTV camera guarding the entrance of a home and also filming some areas of the public space the European Court of Justice ruled that the collected data cannot fall

[653] Davis III, E.F., Alves, A.A., Sklansky, D.A. (2014) Social media and police leadership: Lessons from Boston, *New Perspective in policing,* available online at: http://www.hks.harvard.edu/content/download/67536/1242954/version/1/file/SocialMediaandPoliceLeadership-03-14.pdf (last accessed: 24.3.2016); Cassa, C.A., Chunara, R., Mandl, K., Brownstein, J.S. (2013) Twitter as a sentinel in emergency situations: Lessons from the Boston Marathon explosions, *PloS Currents*, doi: 10.1371/currents.dis.ad70cd1c8bc585e9470046cde334ee4b

[654] Starbird, K., Maddock, J., Orand, M., Achternam, P., Mason, R.M. (2014) Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing, *iConference 2014 proceedings*, available online at: https://hdl.handle.net/2142/47257 (last accessed: 24.3.2016)

[655] Stamp, G. (2011) English riots: Social media were "force for good", *BBC News*, 15 September 2011, available online at: http://www.bbc.com/news/uk-politics-14931010 (last accessed: 24.3.2016)

[656] Rawlinson, K. (2015) National emergency? Belgians respond to terror raids with cats, *The Guardian*, 22 November 2014, available online at: http://www.theguardian.com/world/2015/nov/22/national-emergency-belgians-respond-with-cats (last accessed 8.2.2016)

[657] Lee, D. (2013) Boston bombing: How internet detectives got it very wrong, in *BBC News*, 19 April 2013, available online at: http://www.bbc.com/news/technology-22214511 (last accessed: 12.2.2016)

[658] The judgements of the European Court of Human Rights in cases: M.M. v. The Netherlands, ECHR application no. 39339/98, 8 April 2003, para. 42; A. v. France, ECHR application no. 14838/89, 23 November 1993, para. 38-39 can be extended per analogy to such situations

[659] Directive 95/46/EC

under the exception[660] of the purely personal or household activity and are therefore falling under the general data protection legislation.[661] This reasoning was because of the fact that the CCTV camera was filming also parts of the public space. In situations in which individuals surveil their peers, per analogy with the reasoning of the *Rynes* case, the responsibility will fall not on the State, but on the individuals which qualify in such cases as data controllers. They need to evaluate such a responsibility before engaging in voluntary surveillance activities. In the absence of publication or information on the surveillance result it is difficult, however, for the surveilled individuals to learn that they have been reported by their peers to law enforcement authorities and to act for safeguarding their rights. They are therefore left unprotected.

4.3.3 Challenges to the right to privacy

After discussing the relevance of smartphones for the surveillance activities of law enforcement authorities in the previous section, this section discusses the challenges that surveillance of individuals via smartphones presents for the protection of their right to an undisturbed private life. It was already seen that smartphones create the possibility for dataveillance via access to a large amount of data that are stored in the device, are available via providers or third parties, as well as for direct surveillance when the data are collected on the spot and serve for creating circumstantial evidence. Surveillance mandates have to take all these possibilities into consideration. EU legislation, thus far, while regulating the processing of personal data and the protection of privacy in the electronic communications sector, explicitly excluded from the regulation activities that fell in the areas of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.[662] With the new reformed Data protection package the field will be covered by the general rules of Directive 2016/680. This sub-section will first discuss the challenges that surveillance of individuals via smartphones creates for the issuing of proportionate surveillance mandates and subsequently will focus briefly on the three identified challenges of surveillance with non-purpose built technology: incidental surveillance, mass surveillance and retroactive surveillance.

a) Possibility to interfere with different sets of data – a proportionate surveillance mandate

As already seen above, surveillance via smartphones is not only leading to interception of communications but also to the possibility to searching remotely the device which enables the search of the data stored in it, and to the possibility for direct surveillance. Direct surveillance via smartphones can take place, for example, in those cases in which the GPS sensor of a device is used for tracing the location of an individual, or when the light sensor is used for establishing if the individual is indoors or outdoors, not to mention interception of communications, etc. Dataveillance, on the other side, gives the possibility for access to an enormous amount of metadata and other personal data that might give the possibility for accurate profiling and for drawing maps into the life,

[660] Directive 95/46/EC, article 3(2)
[661] Case C-212/13 Rynes EU:C:2014:2428, para. 33
[662] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Art. 1(3)

activities and interests of the individual. These other personal data might in certain cases qualify even as biometric data[663] (as it is the case with pictures or with the speed of keystrokes)[664] allowing for unique identification of the individuals. The above description shows how heterogeneous the data potentially accessed in case of smartphone surveillance are. The different level of intrusion into the individuals' private life as well as the different safeguards for cases of surveillance of individuals with each of these data make the issuing of proportionate surveillance mandates a challenge for the protection of the right to privacy.

Communication metadata, for example, are already discussed in several cases at the European Court of Human Rights and even at the European Court of Justice. In *Malone*[665] for metering data and in *Copland*[666] with regards to internet communications and surveillance of personal internet usage, the European Court of Human Rights has established that the same level of protection under Article 8 ECHR as in cases of interception of communications content data applies. The invasion of privacy of individuals via collection of communications metadata was recognized also by the Court of Justice of the EU which invalidated the Data Retention Directive for not complying with the proportionality principle.[667]

With regards to the use of a GPS device the European Court of Human Rights finds location tracing in public areas less intrusive and therefore having less strict requirements for a surveillance mandate, than video and audio surveillance[668] and also than interception of communications.[669] The different level of requirements might create situations in which a surveillance mandate issued for the surveillance of one type of data is used for accessing also other available data.

Interception of communications, communications metadata and location tracing are not the only ways the life of the individuals can be intruded via smartphones. There are also other personal data accessible that cannot automatically fall under the category of communications data. These data are not the result of a communication with a communication partner but derive from other activities, as for example an internet search or other activities captured by sensors.

[663] For a definition of biometric data see: Jasserand, C.A. (2015) Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective, *International Data Privacy Law*, pp. 1-14

[664] Banerjee, S., Syed, Z., Bartlow, N., Cukic, B. (2015) Keystroke recognition, in. Li, S.Z, Jain, A.K. (eds.), *Encyclopedia of Biometrics*, pp. 1067-1073

[665] Malone v. The United Kingdom, ECHR application no. 8691/79, 2 August 1984, para. 84

[666] Copland v. The United Kingdom, ECHR application no. 62617/00, 3 April 2007, para. 41; on data protection issues related to search engines see Article 29 Working Party (2008) Opinion 1/2008, 4 April 2008

[667] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland EU:C:2014:238, para. 34

[668] Uzun v. Germany, ECHR application no. 35623/05, 2 September 2010, para. 68

[669] Uzun v. Germany, ECHR application no. 35623/05, 2 September 2010, para. 72

Light sensors, for example, create the possibility for direct surveillance and for identifying the circumstances in which an individual operates (if being indoors or outdoors, in a lighten or dark space). The obtaining of such a valuable information would have probably required otherwise a surveillance measure that would have authorized for a physical search warrant. Physical surveillance would have been the case also with regards to remotely accessing other data from the device as in the cases of activating the video or microphone sensors. A house search warrant would have been necessary in the absence of the technology that allows for remote access to the device data and functions.[670] Even though the inviolability of the home and the house search mandate are seen in general as having very high safeguards for the individuals, there is a difference with regards to remote device searches. In cases of home search the individual learns on the activity of the law enforcement authorities, while in cases of remote access to his device he is per definition unaware of the activity and as a result also less in a position to protect his rights in case of an abuse. Depending from the form of surveillance and the data accessed, smartphone surveillance might thus be very intrusive. In this light, (remote) routine searches of devices (that are lately often claimed)[671] would qualify as unlawful from a protection of privacy prospective.

The issuing of a surveillance mandate for smartphones, for being proportionate, must therefore keep in mind the possibility of access to different categories of data which have as a result different interferences into the private life of the individuals. The request must specify the type of data that will be accessed and the method used for limiting any surveillance activity to such data. The authorities need such information for issuing a surveillance mandate which is in compliance with fundamental rights. An assessment of the impact that the chosen surveillance method will have into the private sphere of the individuals concerned is preferable for a proportionate decision. In case there is the possibility that more than one category of data will be accessed, wilfully or accidentally, (communication content data, metadata, biometrics, location tracing, circumstances, etc.) the most restrictive requirements for issuing a surveillance mandate, as in cases of home searches, must be used.

b) Incidental surveillance

In this study the challenge that incidental surveillance presents to the protection of the private life of individuals was first identified in the case of interception of communications.[672] Surveillance of individuals via smartphones presents the same challenge. Incidental surveillance is seen as the accidental collection of data on individuals that are not the target of the surveillance activity and mandate. With regards to smartphones, the reduced dimensions of the device and its portability create lots of possibilities for its temporary use from third parties, interventions into the device, as

[670] Abel, W. (2009) Agents, Trojans and tags: The next generation of investigators, *International Review of Law, Computers and Technology*, vol. 23, no. 1-2, pp. 99-108

[671] Nelson, F. (2014) Every 73 seconds, police use snooping powers to access our personal records. Who'll rein them in?, *The Spectactor*, 11 October 2014, available online in: http://www.spectator.co.uk/2014/10/now-its-the-police-snooping-in-your-mobile-phone/ (last accessed: 24.2.2016)

[672] Kruslin v. France, ECHR application no. 11801/85, 24 April 1990

well as cases of break and theft. The properties of the device, on the other side, create possibilities for incidental surveillance that go beyond the mere interception of communications.

A remote video or microphone activation of the smartphone, for example, creates enormous possibilities for putting third parties on the spot. This is not only the case when the person under surveillance interacts with other individuals, since this is a normal outcome of a surveillance measure. But there are cases in which other individuals, linked or not linked with the surveilled individual, are by accident in the area covered by the receiving capability of the camera or of the microphone of the device. As a result, they are subject of surveillance without a mandate for their case.

Also remote access to a smartphone device creates possibilities for incidental surveillance. In such cases a "remote forensic software tool" is planted on the device without the knowledge of the owner.[673] There are two main methods for doing this. The first one is by sending malware (viruses and Trojans) via e-mail to the person under surveillance. The access to the e-mail would infect the device and give the possibility for remote access to law enforcement authorities. In case the individual accesses the e-mail account in a device that it is not his then this device is automatically infected and the privacy of a third person would be intruded incidentally. The second method for installing malware is by infecting a website that the suspect is likely to visit. In such a case, also all visitors to the website will be indiscriminately infected by the malware with the possibility for incidental surveillance.

The incidental surveillance of third parties has relevance for the protection of their private life as well as for the accuracy of the data that law enforcement can access when relying on smartphones. Let's think of the example of location tracing. The GPS sensor of the device gives an accurate location estimation. This is known however also by suspects. There have been cases in which the surveilled individual intentionally leaves the device with a different person or sends it around the city with (let's say) the means of public transport for supporting a certain alibi.

The challenge that incidental surveillance creates to the protection of the right to privacy is linked with the reduced possibilities that it offers to individuals for safeguarding their right. Incidentally surveilled individuals are most of the time unaware and uninformed about the interference with their private life and thus also unable to challenge the validity of any surveillance measure.

c) Mass surveillance

[673] Abel, W. (2009) Agents, Trojans and tags: The next generation of investigators, *International Review of Law, Computers and Technology*, vol. 23, no. 1-2, pp. 99-108

There is evidence of the use of smart phones from intelligence and law enforcement authorities for mass surveillance purposes.[674] Intelligence teams in the US and the EU have been reported to unlock the codes[675] and collecting voice, sms and geo-locations as well as the additional functionalities that come with smartphones, such as e-mails, internet searches and social media posts. The British GCHQ is reported to be able also to attack hundreds of applications and to have found ways of looking at the search patterns, e-mails and conversations on many commonly used phone services.[676] Tempora (upstream surveillance activities), Edgehill (the decryption programme), Quantumtheory and Foxacid (the targeted "man-in-the-middle-attacks" on information systems), Dishfire (collecting and retaining 200 million text messages per day) are just a few of the highly technologically advanced systems designed by intelligence services to collect communication data of citizens in a massive and non-suspicion-based manner.

Even though these systems have the aim of increasing State security and to help preventing terrorist attacks, they have to operate in conformity with the rule of law respecting the fundamental rights of the citizens as embedded in the EU treaties[677] and the ECHR.[678] In a resolution of March 2014 the European Parliament goes even further in considering secret and untargeted mass surveillance programmes as being incompatible with the principles of necessity and proportionality in a democratic society.[679] The undesired result of politics overruling the rule of law with regards to mass surveillance programmes was denounced in another resolution of the European Parliament in October 2015.[680]

As already seen above, some types of personal data that can be collected via smartphones could have not been collected without a physical surveillance or a home search. Mass surveillance that allows the collection of such data would be the equivalent of routine intrusions into the homes of individuals. This kind of interference with the private life of non-suspected individuals has to be avoided in a democratic society.

[674] Bigo, D. et al. (2014) Study on the National programmes for mass surveillance of personal data in the EU Member States and their compatibility with EU law

[675] BBC (2013) US NSA and UK GCHQ 'can spy on smartphones', 23 September 2013, available online at: http://www.bbc.com/news/world-europe-24009342 (last accessed: 8.2.2016)

[676] MacAskill, E. et al. (2013) GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications", *The Guardian*, 21 June 2013, available online at: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (last accessed: 8.2.2016); MacAskill, E. et al. (2013) Mastering the internet: how GCHQ set out to spy on the world wide web, *The Guardian*, 21 June 2013, available online at: http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet (last accessed: 8.2.2016)

[677] C-300/11 ZZ v. Secretary of State for the Home Department EU:C:2013:363, para. 38

[678] Parliamentary Assembly of the Council of Europe (2015) Resolution 2045(2015) on Mass surveillance; Parliamentary Assembly of the Council of Europe (2015) Recommendation 2067(2015) on Mass surveillance

[679] European Parliament (2014) Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 2013/2188(INI), para. 5 (main findings)

[680] European Parliament (2015) Resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens, 2015/2635(RSP)

Mass surveillance of smartphone data, apart privacy and data protection problems might create also problems of jurisdiction for cross-border searches. These problems can present themselves in two forms. (i) There is the possibility that smartphone users are temporarily in other jurisdictions carrying their mobile devices with them. In such cases, national authorities carry their surveillance activities in other States without an authorization. (ii) There are cases in which mass surveillance is used, for example, for establishing who is present in a certain square.[681] In such cases there is the eventuality that the location of foreign citizens is also detected. As analysed by Abel (2009), without the consent of the other State involved, such surveillance would be a violation of international law and, maybe even of public international law.[682]

Even if supported by many States, there is not yet any clear evidence on the positive effect that mass surveillance has for State security and the prevention of terrorist attacks. Quite on the contrary, former surveillance experts support the idea that the enormous amount of data collected makes it impossible for experts to make their assessments. Mass surveillance is therefore seen as not giving the results for which it is introduced[683] while putting at the same time most of the private life of individuals under State scrutiny. An evaluation of the necessity and proportionality of any mass surveillance measure would therefore help to bring any interference with the fundamental rights of the individuals under the legality shield. This requirement, one can argue, is also the outcome of the judgement on the invalidation of the Data Retention Directive from the European Court of Justice which has set the presence of necessity and proportionality as a legal requirement for any measure involving massive collection and access to personal data.[684]

d) Retroactive surveillance

Surveillance via smartphones creates possibilities for retroactive surveillance from law enforcement authorities. This is linked with the periods of retention of different types of data that are generated in the smartphones. The retention of these data can have different reasons and justifications. This might be the result of legislation, of retention by service/network providers or other parties, as for example providers of applications, of the design of the device or even of the smartphone users themselves. Each possibility will be briefly discussed below in turn.

i. Data retention legislation

[681] King, E. (2012) Civil servant admits British police grabbing location data of thousands of innocent people, available online at: https://www.privacyinternational.org/blog/civil-servant-admits-british-police-grabbing-location-data-of-thousands-of-innocent-people, (last check: 18.07.2013)
[682] Abel, W. (2009) Agents, Trojans and tags: The next generation of investigators, *International Review of Law, Computers and Technology*, vol. 23, no. 1-2, pp. 99-108
[683] O'Cleirigh, F. (2016) French intelligence 'could have prevented Paris attacks', in Computer Weekly, available online at: http://www.computerweekly.com/news/4500270121/French-intelligence-could-have-prevented-Paris-attacks (last accessed 10.2.2016)
[684] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland EU:C:2014:238

As already discussed in chapter 2 the European legislation on retention of communications' metadata was invalidated in April 2014.[685] The invalidation of the Directive does not mean, however that national rules on the subject are automatically invalid. In the absence of harmonized rules Member States can maintain their national laws or even adopt new legislation dealing with data retention for as long as they comply with the basic principles of EU law, the e-Privacy Directive and the judgement of the Court.[686] Some Member States have currently still in life their data retention regimes, despite the fact that it was adopted as the result of the implementation of the now invalidated Data Retention Directive.[687] Other Member States were invalidating their rules[688] and others have introduced or are in the process of introducing new data retention laws.[689]

On the basis of the data retention legislation service providers have to retain metadata from communications for established periods of time and to make them available to law enforcement authorities that are investigating serious crimes. These metadata include information that enables the identification of the source and the destination of the communication, the date, the time, the duration, the type of communication, the device and its location.

ii. Retention of data by service/network providers or other parties

Personal data from communications are retained also from the phone providers themselves for different purposes as for example billing or marketing. The same applies also for providers of applications. For the later even though there are indications and evidence that they collect personal data from smartphone users there is not a clear study showing the extension of their data collection activity, what they do with the data and in how far their collection regards content data from communications.[690]

iii. Retention of data by the device

As stated earlier smartphones are a combination of phone technology with computing capabilities. This creates the possibility for the memory of the device itself to store data. These data might be retrieved retroactively even if the user thought that he was deleting them.

[685] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland EU:C:2014:238

[686] European Commission (2015) European Commission statement on national data retention laws, 16 September 2015, Statement/15/5654

[687] EDRi (2015) Non-exhaustive list of EU Member States with national legislation contrary to the Digital Rights Ireland Ltd (C-293/12) CJEU ruling, available online at: https://edri.org/files/DR_EDRi_letter_CJEU_Timmermans_20150702_annex.pdf (last accessed: 11.2.2016)

[688] For the Netherlands see: RBDHA 11 March 2015 ECLI:NL:RBDHA:2015:2498 (Stichting Privacy First et al. t. de Staat der Nederlanden); for France see: Arrêt no. 84/2015 du 11 juin 2015

[689] For the UK see: Data retention and Investigatory powers act 2014; for Germany see: Reichert, C. (2015) Germany moves closer to data retention, in *ZDNet*, 19 October 2015, available online at: http://www.zdnet.com/article/germany-moves-closer-to-data-retention/ (last accessed: 11.2.2016)

[690] Shklovski, I., et al. (2014) Leakiness and creepiness in app space: perceptions of privacy and mobile app use, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2347-2356

iv. Retention of data by the smartphone user

Lastly, the smartphone user might save different personal data on his device. These can be contacts, passwords, pictures, videos, etc. giving the possibility to law enforcement authorities to retrieve these data retroactively.

The duration of the period of data retention gives the possibility to surveil the life of the individuals retroactively, including periods of time in which he was not yet a suspect. As seen above because of their design, legal requirements or other reasons smartphones facilitate this form of surveillance which challenges the protection of the right to privacy.

4.3.4 Concluding remarks

Smartphones are the second case study of this research. They are a good representation of non-purpose built devices which are currently extensively used for surveillance purposes. The section showed the current use as well as potential future uses of these devices by law enforcement authorities. It was seen that smartphones give possibility for ubiquitous surveillance. They allow for the performance of different forms of surveillance and they also give access at the same time to a large number of heterogeneous types of personal data, from metadata to biometrical data. The interference that surveillance via this technology has into the private life of the individuals is thus not limited to the area of private communications.

The way smartphones are designed and operate makes surveillance easily performed not only by other private parties but also by law enforcement authorities that operate for ensuring the security and safety of individuals and of the States. Even though there is no special legislation on surveillance via smartphones, the human rights legislation in the EU requires that the easiness in performing surveillance must not compromise the protection of the rights to privacy and data protection of the individuals. It must not come as a surprise therefore that the first suggestion for safeguarding the rights of the individuals is linked with the design of the device. If the protection of privacy is introduced as a design future of the device this would make surveillance activities more difficult and preferably also less frequent.

Protection of privacy as a design future of the device would certainly reduce interferences with this right from private parties and also reduce State surveillance without leaving the devices outside the reach of law enforcement. It is enough to remember here that with the advancement of telephony technology from analogue to digital, telephone companies and providers were required to create the law enforcement possibility for intercepting communications as one of the futures of their devices and systems. The introduction of data retention legislation in the EU even required service providers to build capabilities to retain the data in compliance with the legal rules. In the same fashion, the protection of privacy as a design future of the device can be accompanied by rules that insure the

possibility for law enforcement to use the device for surveillance activities in specific individual cases (as for example the availability of decryption codes in cases of encryption).[691]

The developing of forms of encryption from smartphone producers for Apple and Android devices has, however, not been well received by law enforcement (at least in the US).[692] Though encryption is seen as a way to protect individuals from unlawful interferences with their private lives from other private parties, it influences also the success of warrantless mass surveillance from State authorities. As stated in a number of reports from the European Parliament, smartphones are currently used in surveillance activities that are kept secret and that bar the individuals of the possibility to safeguard their rights. The existence of decryption capabilities must however be linked to specific cases and not have the effects of an overall decryption that would potentially jeopardize the right to privacy of all users of a specific technology.[693]

There are not yet clear and public statistics on the positive effects that mass surveillance of communications has brought to the States' law enforcement and intelligence activities. The proportionality of such a form of surveillance as well as the active State sponsoring for the development of technologies for cracking communications[694] can thus be questioned from a protection of human rights point of view.

Currently, since there are no specific rules for surveillance via smartphones in place, the general surveillance rules apply for analogy. These rules are designed with old generation technology in mind. The advanced technology, however, allows for heterogeneous types of personal data to be accessed within one device and on the basis of the same surveillance mandate. The obtaining of some of these data, in the absence of technology, would require for a mandate for home or physical search. Rules should therefore be in place to regulate such situations while safeguarding the protection of the fundamental rights of the individuals.

---

[691] Against the access of decryption codes by law enforcement see the conflict between FBI and Apple - Hern, A. (2016) Is the FBI v Apple PR war even about encryption?, in *The Guardian*, 23 February 2016, available online at: http://www.theguardian.com/technology/2016/feb/23/fbi-apple-pr-war-encryption-mobile-security (last accessed: 11.3.2016) – and the 16 February 2016 open letter to customers from Tim Cook, Chief executive of Apple Inc., available online at: http://www.apple.com/customer-letter/ (last accessed: 11.3.2016)

[692] See speech of J. B. Comey, director at FBI, available online at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (last accessed: 15.2.2016); Timberg, C., Miller, G. (2014) FBI blasts Apple, Google for blasting FBI out of phones, in The *Washington Post*, 25 September 2014, available online at: https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html (last accessed: 15.2.2016)

[693] See the statement of the UN High Representative on Human Rights, 4 March 2016, available online at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E (last accessed: 11.3.2016)

[694] Rosenbach, M., Poitras, L., Stark, H. (2013) iSpy: How the NSA Accesses Smartphone Data, in *Der Spigel,* 9 September 2013, available online at: http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html (last accessed: 22.2.2016)

The remote access to computers of suspects as a surveillance measure in the case of cybercrimes is recognized and recommended also by the Council of the European Union.[695] However no safeguards for the individuals are designed thus far at European level. The regulation is left in the hands of the national legislators. In this light the Federal Constitutional Court in Germany[696] argued the creation of a "*fundamental right to the guarantee of the confidentiality and integrity of information technology systems*" in those cases in which intrusion into information technology systems is either not protected at all or not properly protected by other fundamental rights, as for example the right to inviolability of the home, secrecy of communications, etc.[697] The decision of the German Federal Constitutional Court is inspired by the need to protect the fundamental rights of the citizens in light of technology advances that are not yet covered by the laws. The outcome of the case might serve as a starting point also for the European regulator to introduce harmonized rules for remote access into devices with computing capabilities. Harmonised rules will serve to regulate also cross-border situations that present a conflict of jurisdictions due to the fact that the surveillance measure might easily extend to periods of time in which the individual is not in the country and carries his device with him in other Member States.

In addition, a method for assessing the surveillance properties and privacy implications of the use of smartphones for surveillance purposes is needed to ensure the proportionality of the surveillance mandate. This method would guide the decision-making process of national authorities that issue surveillance mandates to identify the implications with regards to the aspects of the private life of the individual that are being interfered with, the level of interference, as well as the interference with the life of third parties.

4.4 Stand-alone portable GPS devices

The third case study addresses stand-alone portable GPS devices, the use of which for surveillance purposes creates interference with the privacy of location and space which is one of the most recent recognized aspects of privacy. Currently the EU law lacks a general definition of "location data". The only one that could be found is in Directive 2002/58/EC, article 2(c), which defines location data as: "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*."[698] This definition is limited to locations that can be tracked due to publicly available electronic communication services. It explicitly excludes information society services, as for example the satellite based Global Positioning technology (GPS) that is one of the most prominent examples of

[695] Council of the European Union (2008) Council conclusions on a concerted work strategy and practical measures against cybercrime, 2987th Justice and Home Affairs Council meeting, 27-28 November 2008
[696] Federal Constitutional Court, Decision of February 27, 2008, BVerfG, NJW 2008, 1 BvR 370/07
[697] Wiebe, A. (2008) The new fundamental right to IT security – first evaluation and comparative view at the U.S., *Datenschutz und Datenschicherheit*, vol. 32, no. 11, pp. 713-716; Togias, S. (2011) The right in confidentiality and integrity of information technology systems according to the German Federal Constitutional Court: "Old wine in new bottles?", in Kanellopoullou, M.M. (eds.), *An information law for the 21st century*, pp. 530-540
[698] A terminal equipment according to this definition is, for example a smartphone

technology that interferes with the privacy of location and space.[699] Also the new reform package on data protection does not include a definition of location data.

Following this short introduction, in sub-section 4.4.1 is presented some background information on GPS navigation devices. In sub-section 4.4.2 is discussed the personal nature of GPS navigation data. In sub-section 4.4.3 are presented actual and potential uses of GPS devices by law enforcement authorities. In sub-section 4.4.4 are discussed the protection of privacy in the public space (4.4.4.1) and are assessed the challenges that surveillance of individuals via GPS devices creates for safeguarding the right to privacy (4.4.4.2). The conclusions are presented in sub-section 4.4.5.

4.4.1 Background information on GPS navigation devices and on the data that they collect

The Global Positioning System is designed with the original aim to calculate the positioning, the velocity and the precise coordination of time for any device furnished with a GPS receiver. The system is conceived as a ranging system from known positions of satellites in space,[700] each rotating in one of the 6 different orbits around the earth, to unknown positions on land, sea, air and space.[701] Each satellite transmits a radio signal. The location of a device is determined when at least 4 of these signals are captured by its in-built GPS sensors.[702]

This technology was first developed in the framework of the US Air Force for military purposes in the 1960s. For civilians, the GPS technology was commercially released in 1995 though it was only after the year 2000 that consumers could have the same level of accuracy of the service as the military forces.[703] From that year onwards devices furnished with GPS technology, which is relatively inexpensive, have proliferated.

This case study focuses on stand-alone GPS devices for car navigation. These devices have in the recent years become indispensable travel companions for many drivers.[704] In their design GPS car navigators support the driver by showing the car's location on a map and by giving both visual and

[699] Bajaj, R., Ranaweera, S.L., Agrawal, D.P. (2002) GPS: Location tracking technology, *Computers*, vol. 35, no. 4, pp. 92-94
[700] For the European Galileo global satellite navigation system see: http://ec.europa.eu/growth/sectors/space/galileo/ (last accessed: 13.4.2016)
[701] Hofmann-Wellenhof, B., Lichtenegger, H., Collins, (1997) Global Positioning System: Theory and Practice, Springer, 4th edition, p. 11
[702] Article 29 Data Protection Working Party (2011) Opinion 13/2011 on Geolocation services on smart mobile devices, 16 May 2011
[703] Michael, K., McNamee, A., Michael, M.G. (2006) The emerging ethics of humancentric GPS tracking and monitoring, in *Proceedings of the International Conference on Mobile Business*, pp. 34-42
[704] Canalys (2006) Research Release 2006/81: Mobile GPS navigation market doubles year-on-year, available online at: http://www.gpsforensics.org/downloads/canalys_11aug06.pdf (last accessed: 21.4.2016)

audio information on how to efficiently get from one location to another, to plan routes, to save favourite locations, to look up for points of interest, etc.[705]

GPS navigation devices come, however, with a downside. They do not only assist drivers but also track their location and movements in the public space by collecting data which are accessible by the GPS device companies, car builders or other service providers.[706] With regards to the collection and the access to the data activity by service providers, Jim Farley, top sales executive at Ford Motor Company, speaking at a panel at the international CES 2014 conference, said: "*We know everyone who breaks the law. We know when you are doing it. We have GPS in your car, so we know what you are doing*."[707]

The data collected are related with the past or current locations on a map, the routes in which the device has been and the itineraries that it has calculated in the past, the saved preferred destinations such as the home address, the speed with which the device has travelled at any point in time and space, etc. The processing of these data creates possibilities even for predicting future locations of the device.[708]

The GPS service providers can acquire the geolocation data historically or on real-time. Historical data are collected from offline versions of devices when the device is connected with the servers, for example to install new maps.[709] Until the connection of the device with servers, the data are saved in the device itself. Real-time data are collected from online versions of GPS navigation devices with short time intervals (three minutes) which creates the possibility for accurate surveillance and predictions.[710]

The collected data are retained from the service providers for periods of time which are not transparent. In an opinion of the Article 29 Working Party, for complying with the EU data protection

[705] Skog, I., Handel, P., (2009) In-car positioning and navigation technologies – A survey, in *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 1, pp. 4-20

[706] In this chapter, GPS device companies, car builders or other service providers are referred in general as 'service providers'

[707] Tropjan, C. (2014) The next data privacy battle may be waged inside your car, *The New York Times*, 10 January 2014, available online at: http://www.nytimes.com/2014/01/11/business/the-next-privacy-battle-may-be-waged-inside-your-car.html?_r=0 (last accessed: 12.4.2016)

[708] Ashbrook, D., Starner, T. (2003) Using GPS to learn significant locations and predict movement across multiple users, in *Personal and Ubiquitous computing*, vol. 7, pp. 275-286

[709] Many users of GPS devices connect regularly to the online services for updating their software. The TomTom company, for example, states that the majority of users in the Netherlands use the software update within two to three months. This estimation includes for the offline devices

[710] CBP (2011) Official investigation by the CBP into the processing of geolocation data by TomTom N.V., public version available online at: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20120112_investigation-tomtom.pdf (last accessed: 13.4.2016)

legislation, providers of GPS services are advised to retain the collected data only for justified periods of time that are linked with the purpose of collection.[711] Since the data are mainly said to be collected for improving the quality of the product and of the service, it is difficult to determine what a justified period of time is and this estimation is left with the service provider itself. In the following sub-section is discussed the qualification of GPS data as personal data.

4.4.2 GPS navigation data under EU data protection and privacy rules

Even though thus far GPS navigation data are referred as related with a device, is submitted that these data qualify as personal data under EU law.[712] As defined in article 2(a) of Directive 95/46/EC, personal data is any information that relates to an identified or identifiable natural person. An identifiable person is the one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Further, in recital 26 of Directive 95/46/EC it is explained that to determine whether a person is identifiable account should be taken of all the means likely and reasonably to be used either by the controller or by any other person to identify the said person.

With regards to GPS navigation devices there are different ways to link the tracked device with an identified person. The first method is related to the fact that GPS companies hold files in which the serial number of the device is held together with identifying data of the owner (such as the name, e-mail address, telephone number, etc.). With regards to one of the largest GPS navigation companies, TomTom, identifying data of the owner of the device are kept when:

a. the device was purchased via the web shop;
b. the purchaser used a discount or exchange promotion;
c. the user contacted the customer service and/or technical support;
d. the user creates an account which is linked to the device.[713]

Secondly, it is possible to combine the navigation data with other databases, as for example the ones from automatic number plate recognition and the ones from the vehicle registry. With this method it is possible to link the GPS navigation data with an individual identified as the owner of the vehicle.

[711] Article 29 Data Protection Working Party (2011) Opinion 13/2011 on Geolocation services on smart mobile devices, 16 May 2011
[712] Hildebrandt, M. (2014) Location Data, Purpose Binding and Contextual Integrity: What's the Message?, in Floridi, L. (eds.) *Protection of Information and the Right to Privacy - A New Equilibrium?*, pp. 31-62
[713] CBP (2011) Official investigation by the CBP into the processing of geolocation data by TomTom N.V., public version available online at:
https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20120112_investigation-tomtom.pdf (last accessed: 13.4.2016)

The linking of the data with an identified or identifiable person as in the above two methods might not be accurate. The use of the first method has the consequence that the data are linked to the person that is the official purchaser or that normally is in charge of updating the GPS device, while might be other members of the family or other parties that are making use of it. The same concern may arise also with the use of the second method which links the data to the official owner of the vehicle which in practice might be used by another person. In these cases, even though the navigation data are linked to an identified or identifiable person the accuracy of this link has a large margin for error.

For minimizing this error the method presented below is more appropriate for linking the data. The collection of the data and their indeterminate period of retention creates the possibility for profiling while linking with databases that are more accurate with regards to their reference to a specific individual (as are for example smartphone data). This method gives the possibility for separating the data and for linking them to specific users of the vehicle and of the device. It gives the possibility for establishing the location and movements of identified or identifiable individuals with more accuracy than in the first and second case. The presence of more than one person in the vehicle does not compromise the qualification of the data with regards to the interference with the privacy of location and space since the data are valid for any of these individuals separately. Some more profiling might be needed, though, for identifying the driver of the vehicle at a specific point in time when the data are linked with more than one individual.

Independent from the possibility of errors, all three methods create the possibility for linking the GPS navigation data to identified or identifiable individuals. The data do, therefore, fall under the protection of the European data protection rules.

4.4.3 GPS navigation data for law enforcement authorities

After presenting some background information on the development of the GPS technology and of the data that GPS navigation devices collect, this sub-section will discuss present and potential uses of the device by law enforcement authorities for surveillance purposes. As already seen in the previous section GPS navigation devices create the possibility for the collection of historical data (dataveillance) as well as for real-time (direct) surveillance. Both possibilities have relevance for law enforcement authorities. They can access the data directly from a confiscated device (that functions offline), from the service provider or they can even remotely activate such a functionality.[714]

On the basis of GPS historic data, law enforcement can learn itineraries of an individual as well as his preferred destinations. Locations can be determined in specific points in time and there is the

[714] Cavoukian, A. (2013) Surveillance, then and now: Securing privacy in public spaces, available online at: https://www.ipc.on.ca/images/Resources/pbd-surveillance.pdf (last accessed: 26.4.2016)

possibility to learn about driving behaviour, the driving speed at specific points in time, habits, etc.[715] The data can be used for building hypothesis or for verifying alibies.[716] These data, combined or not with data from other databases such as the vehicle registration system or from the mobile phone, is in practice regularly used as evidence by the law enforcement.[717]

The collected data create also the possibility for generating profiles. One can establish for how long one stays at home, or at work, the addresses, the hours one works, etc. It needs little imagination to identify the private nature of trips to a specialist clinic, to the mosque, synagogue or church, to a motel and so on. The data can be correlated with other persons' location data to even infer social networks, at least with some probabilistic confidence.[718] Data are capable of being linked with other sources for the scope of individual surveillance (of a suspect), or even for mass surveillance (in order to generate suspects). In general, the value of any information increases when it is related to a location and a location, on the other side, might be the first clue for categorizing and labelling.[719] The knowledge that an individual has visited a location, may reveal other information such as: political interests, personal interests, circle of friends or acquaintances, health problems, etc.

Online GPS navigation devices give the possibility for real-time surveillance of the location and whereabouts of an individual. Triangulation by multiple satellites locates the device and thus also its user[720] making GPS the most accurate method for finding locations in the open spaces.[721]

There are already examples in which GPS navigation service providers have made use and transferred to third parties data collected with this technology. The most prominent example is the one of the Dutch company TomTom. In 2011, the company, in return for payment, was transferring directly or indirectly data collected from the users to third parties, such as local and provincial authorities,[722] the Eindhoven Airport and a traffic advice office (Via.nl).[723] The data were further transferred to the law

[715] Michael, K., McNamee, A., Michael, M.G., Tootell, H. (2006) Location-based intelligence - Modeling behavior in humans using GPS, Proceedings of IEEE International Symposium on Technology and Society, pp. 1-8

[716] Wainright, R. (2007) Father and son stick to guns to prove radar wrong, *Sidney Morning Herald*, 12 March 2007, available online at: http://www.smh.com.au/news/national/father-and-son-stick-to-guns-to-prove-radar-wrong/2007/03/11/1173548023012.html (last accessed: 21.4.2016)

[717] For some cases decided from courts in the Netherlands in which evidence collected by the GPS navigation system was used see: RBZUT 25 February 2011 ECLI:NL:RBZUT:2011:BP5729; RBHAA 15 September 2010 ECLI:NL:RBHAA:2010:BO2789; RBZLY 6 May 2010 ECLI:NL:RBZLY:2010:BM3601

[718] Wigan, M., Clarke, R. (2006) Social impacts of transport surveillance, *Prometheus*, vol. 24, pp. 389-403

[719] Decker, M. (2008) Location privacy – An overview, *IEEE Proceedings of the 7th Conference on Mobile Business*, pp. 221-230

[720] Tsai, J.Y., Gage Kelley, P., Faith Cranon, L., Sadeh, N. (2010) Location-sharing technologies: Privacy risks and controls, *A Journal of Law and Policy for the Information Society*, vol. 6, no. 2, pp. 119-317

[721] The GPS technology does not work well in closed spaces due to the weak signal

[722] Local and provincial authorities were interested in the GPS navigation data to see how and where traffic jams occur and to take specific measures to improve traffic flows and try to make the roads safer

[723] CBP (2011) Official investigation by the CBP into the processing of geolocation data by TomTom N.V., public version available online at:

enforcement authorities (sometimes for payment), even though not directly from TomTom but from the traffic advice office. Law enforcement used these data for establishing speed traps.[724] "*Dutch drivers might wonder how it was that speed traps were always in just the right place to catch speeders*."[725]

The users traffic data transferred in the above example were anonymous, aggregated and collected on the basis of a consent for collecting anonymous data for improving the quality of the product and service offered. As a consequence, the transferal of the data from TomTom to third parties was not caught by the provisions of Directive 95/46/EC. However, as already seen in the previous section, there are different possibilities for TomTom itself as well as for law enforcement authorities to link the data with the right individuals. They can do it with the collaboration of the service provider or by linking different databases. Even though individuals were insured that such a possibility was not used in the concrete case, law enforcement might use the data for mass surveillance, penalizing specific violators of traffic rules or even trying to find the whereabouts of specific suspects.

Without technology surveillance of a vehicle for certain periods of time requires a large team of agents, a number of vehicles and may be even aerial assistance. The costs would limit such a practice to investigations of specific importance. The use of GPS navigation devices for surveillance makes such an activity easy and cheap and therefore very interesting for use by law enforcement authorities.

4.4.4 Challenges to the right to privacy

After discussing the possibilities that stand-alone GPS navigation devices create for surveillance of individuals by law enforcement, this section deals with the challenges that this creates to the right to privacy. Even though it was already discussed that the data collected and accessed via GPS devices qualify as personal data, since the data are linked with activities which take place in public spaces the section will first discuss the existence or not of the right to privacy in such situations. Than the possibilities for incidental surveillance, mass surveillance and retroactive surveillance are discussed.

---

https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20120112_investigation-tomtom.pdf (last accessed: 13.4.2016)

[724] Palmer, M. (2011) TomTom sorry for selling driver data to police, in *Financial Times*, 28 April 2011, available online at: http://www.ft.com/cms/s/2/3f80e432-7199-11e0-9b7a-00144feabdc0.html#axzz45th62fsM (last accessed: 15.4.2016)

[725] Arthur, C. (2011) TomTom satnav data used to set police speed traps, in *The Guardian*, 28 April 2011, available online at: https://www.theguardian.com/technology/2011/apr/28/tomtom-satnav-data-police-speed-traps (last accessed: 15.4.2016)

4.4.4.1 The right to privacy in cases of location tracing in public spaces

The right to privacy as defined in article 8 ECHR and article 7 of the EU Charter of Fundamental Rights protects the private sphere of the individuals which seams from the wording of the articles as projected mainly in private spaces (private and family life, home and correspondence). When someone exposes himself in a space that is open to the public he creates the possibility to be visible to others whom have a right to observe what goes on around them. It is, however, one thing to be seen in public and another to be tracked by the State.

The public space creates the possibility for a number of everyday activities which are vital to the normal life of an individual such as: transportation, shopping, socializing, etc.[726] Technology makes it possible, on the other side, to identify more details than the bare eye. In addition, recorded data has a different character from human observation and creates possibilities for further processing of the data by sorting, refining and matching them.[727] The protection of the private sphere of the individuals would not be complete if data collected and recorded about their activities in public spaces are not covered.[728]

As it is discussed further in chapter 5, in Europe the extension of the private sphere of individuals to the public space is to be found in the jurisprudence of the European Court of Human Rights. Since capture of an event changes its nature from a simple observation to a record, it is the systematic or permanent storage of data collected in open spaces as well as their compilation, processing, use or disclosure that makes these data fall under the protection of the right to privacy.[729]

In *P.G. and J.H.* the Court dealt with the scope of the right to privacy in public spaces establishing that: "*There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain*."[730]

---

[726] Patton, J.W. (2000) Protecting privacy in public? Surveillance technologies and the value of public places, *Ethics and Information Technology*, vol. 2, pp. 181-187

[727] Lyon, D. (2003) Surveillance as social sorting: Computer codes and mobile bodies, in Lyon, D. (eds.) *Surveillance as social sorting: Privacy, risk and automated discrimination*, pp. 13-30

[728] Scassa, T. (2009) Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy, *Canadian Journal of Law and Technology*, vol. 7, no.2, pp. 193-220

[729] Nouwt, J. (2008) Reasonable expectation of geo-privacy?, *SCRIPT-ed – A Journal of Law, Technology and Society*, vol. 5, no. 2, pp. 375-403

[730] P.G. and J.H. v The United Kingdom, Application no. 44787/98, 25 September 2001, para. 57

In the same line, the Court confirmed in *Perry* that the right to privacy exists also outside a person´s home or private premises.[731] While a simple viewing of activities, even if aided by technology, without any recording is considered as compatible with the right to privacy,[732] the situation changes as a result of new technologic developments which systematically or permanently record the data.

Driving is a regulated activity and some surveillance and supervision of vehicles and drivers is expected. These activities must, however be reasonable.[733] In *Uzun* the Court concluded that surveillance of an individual in public spaces via a GPS receiver built in the car falls under the scope of application of article 8(1) ECHR even though is to be considered as a less intrusive method than video or audio surveillance.[734]

In the above mentioned case the GPS receiver was built in the car for the purpose of surveilling the movements and locations of Mr. Uzun and his accomplice. It follows, with more reason, that surveillance via stand-alone GPS navigation devices used by individuals with their will and not built for the purpose of surveillance falls as well under the scope of application of article 8(1) ECHR. The use of such technology for surveillance purposes, despite the public space in which it takes place, must follow the rules and safeguards established for the protection of the right to privacy of the individuals.

4.4.4.2 Incidental surveillance, mass surveillance and retroactive surveillance

After establishing that interference with the life of the individuals via GPS navigation devices falls under the protection of the right to privacy, in this sub-section are discussed the challenges created to the right by increased situations of incidental surveillance, mass surveillance and retroactive surveillance. Each of these situations are discussed in turn.

a) Incidental surveillance

Surveillance via GPS devices creates increased possibilities for incidental surveillance of all users of the tracked vehicle or of the device. It was already seen that GPS devices create the possibility for collecting data on the routes, locations, etc. in which the device has been. The linking of data to single individuals comes as the result of profiling and analysing activities. This implies that all the data collected, independent from the individual with whom they are linked, are being analysed and scrutinized. As a result, exists an open possibility for incidental surveillance of individuals that are not

[731] Perry v The United Kingdom, Application no. 63673/00, 17 July 2003, para. 37
[732] Perry v The United Kingdom, Application no. 63673/00, 17 July 2003, para. 38
[733] Cavoukian, A. (2013) Surveillance, then and now: Securing privacy in public spaces, available online at: https://www.ipc.on.ca/images/Resources/pbd-surveillance.pdf (last accessed: 26.4.2016)
[734] Uzun v Germany, Application no. 35623/05, 2 September 2010, para. 52

the target of the surveillance activity by law enforcement. It was already seen that the data might be linked with different individuals as for example the owner of the vehicle, of the device, the driver, the passengers.

As it was seen in chapter 2, the right to privacy of individuals that find themselves in a situation of incidental surveillance is not properly protected in the current European legal framework. Law enforcement use of stand-alone GPS navigation devices for surveillance purposes will, therefore, have as a result that these individuals will be left without proper safeguards for the protection of their right. This consequence has to be taken into account when deciding on the employment of this form of surveillance.

Another element, related with profiling and analysing the data as well as with the possibility of incidental involvement of individuals in surveillance is the accuracy of the data and the possibility for errors. Firstly, errors might occur as a result of the analysing of the data. It exists the possibility that an individual takes a trip that coincides with a route that is normally attributed to another individual. Secondly, it is proved that the positional data stored in the memory of a GPS device can be easily edited with a compatible software tool.[735] As a result, suspicious individuals might corrupt evidence about them or innocent individuals might be caught by GPS data surveillance activities. Thus, the use of GPS data as evidence in legal proceedings might not have the value that it is believed to have while still interfering with the right to privacy of individuals.

b) Mass surveillance

Mass surveillance of citizens via their GPS navigation devices is not a remote possibility. The possibility as well as the interest that law enforcement has for using such data is nicely illustrated in the experience that users of the TomTom navigation device had in 2011 when law enforcement in the Netherlands received and even bought the data from third parties. Even though the data used in such a situation where anonymous, technology provides different ways to link them to identified or identifiable persons. If there is GPS data showing that an anonymous individual was at a specific location at a point in time which has interest for specific investigations, combining those data with, for example, smartphones data would give a first clue for identifying the individual.

Since mass surveillance does not target specific individuals but preventively aims to generate suspects on the basis of objective surveillance criteria, GPS data create good possibilities for this. The data can be used not only for identifying violators of traffic rules but also for creating profiles of individuals linked with their driving behaviour and the locations that they frequent. This last possibility, even if less intrusive than some other forms of surveillance, is still creating serious interferences with the private lives of the individuals.

[735] Iqbal, M.U., Lim, S. (2008) Legal and ethical implications of GPS vulnerabilities, *Journal of International law and Technology*, vol. 3, no. 3, pp. 178-187

As it was already seen in chapter 2 there is no transparency on the existence of mass surveillance programs already operating in the EU and the citizens caught by the activities of these programs do not enjoy a proper protection of their right to an undisturbed private life. Mass surveillance via GPS navigation devices would create a situation of total surveillance of the movements of an individual in the public space as well as of the frequented locations when using a vehicle furnished with the GPS device. The lack of information and proper safeguards makes the individuals vulnerable to this form of surveillance. Such a close and continuous surveillance should require supervision under a system of prior judicial authorization.

c) Retroactive surveillance

There are no laws at European level that require service providers or other parties to retain GPS data for law enforcement or for other purposes. Service providers might, however, retain the data by themselves for the purpose of improving the services that they offer. There is no transparency on this data retention activity and its duration and, as the Dutch data protection authority established in the TomTom case,[736] even if the data are retained as anonymous there is the possibility to link them to identified or identifiable individuals.

Apart the retention of the data for improving the services, there are efforts underway to use GPS vehicle navigation infrastructure for additional value-added services, as for example mobility pricing of insurance, infrastructure-less electronic toll collection or GPS enabled parking fee collection, etc.[737] This might result in even longer periods of data retention from the providers of the service as well as from third parties.

The long periods of data retention create possibilities for going back in time and employing retroactive surveillance which was seen in chapter 2 to create problems not only to the protection of the right to privacy of the individuals but also to the effectiveness of the due legal process in general. The need to analyse historic GPS data for linking them to identified or identifiable persons creates a present and not negligible possibility for retroactive surveillance in cases of individual surveillance.

Mass surveillance on the other side is done per definition in the absence of a specific suspicion. As a result, the private sphere of the individuals is scrutinized in these cases at the time there is not any indication for their involvement in a criminal activity. These problems created to the protection of

[736] CBP (2011) Official investigation by the CBP into the processing of geolocation data by TomTom N.V., public version available online at:
https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20120112_investigation-tomtom.pdf (last accessed: 13.4.2016)

[737] Iqbal, M.U., Lim, S. (2010) Privacy implications of automated GPS tracking and profiling, *IEEE Technology and Society Magazine*, pp. 39-46

the private sphere of individuals must be taken into account by the national authorities issuing a surveillance mandate.

4.4.5 Concluding remarks

Stand-alone GPS navigation devices are a clear example of devices not built for the purpose of surveillance but with a potential to be used for such a purpose. Their design and capability make surveillance of location and movements of an individual using a vehicle in the public space an easy and cheap task for law enforcement authorities. There are already cases in which data from GPS navigation devices are used as evidence in trials.

There are no laws in the EU that prohibit the use of stand-alone GPS navigation data for surveillance purposes. In comparison with the previous two case studies, smart meters and smartphones, one can say that the level of interference that these data have with the private sphere of the individuals is not to be considered as very intrusive because the surveilled activities take place in the public space under the eyes of many viewers. It is only recently, due to technologic advances, that location and space are added to the areas of protection of the private sphere of the individuals. It was seen in this section, however, that the information that can be learned on the private life of an individual from surveillance of his movements in the public space can be very intrusive and information can be gained, for example, with regards to health issues, political or religious associations, etc.

It is not the mere observation, but the permanent or systematic collection that makes such data fall under the European privacy protection rules. The link that the data have to identified or identifiable individuals makes them qualify as personal data and therefore protected also by the EU data and privacy protection rules.

Surveillance of individuals via GPS navigation devices creates challenges to the protection of the right to privacy. The increased possibilities for incidental surveillance, mass surveillance and retroactive surveillance are situations for which sufficient safeguards for protecting the right to privacy are missing and as a result, individuals are exposed to potential infringements of their rights. There is also a possibility for errors as well as for alterations of the data. As a result of these situations that make the individuals vulnerable to an infringement of their rights, in the absence of proper legal safeguards, it is important for the national authorities to carefully assess the necessity and the proportionality of the use of GPS navigation devices for surveillance purposes. Warrantless surveillance of the daily activities of individuals in the public space must be an unthinkable prospect in a democratic society.

4.5 Discussion and conclusion

The possibility of State surveillance with non-purpose built devices and the implications that this presents for the private lives of the individuals was seen in this chapter with the assessment of three case studies: smart meters, smart phones and stand-alone portable GPS devices. Though not built for the purpose of surveillance, these devices have as part of their design the possibility to surveil the activities of their possessors as well as of other persons, incidentally. The easiness with which they can be used in situations of direct surveillance, dataveillance, individual or mass surveillance, and retroactive surveillance is directly linked with their design and capabilities. The employment of such devices in surveillance activities facilitates the work of law enforcement authorities logistically, technically, economically, etc. In using these devices for surveillance, however, the authorities must comply with the fundamental rights to privacy and data protection.

As already discussed earlier in this study, surveillance with non-purpose built technology in the EU is not identified as a special form of surveillance, despite the differences that it presents with traditional surveillance. The use of the same legislation as in cases of traditional surveillance exposes the protection of the rights of the individuals to increased risks for their violation. That is also why the care when issuing surveillance mandates for the use of these devices needs to be increased and specific.

As it was seen from the case studies, devices non-built for the purpose of surveillance but that might be used for such a purpose are everywhere. Individuals that benefit from the amazing advancements of technology use them voluntarily (as in the case of smartphones and GPS devices) or on the basis of legal obligations (as in the case of smart meters). Many of these devices have the possibility to make surveillance ubiquitous, continuous and omnipresent, and they present challenges to the right to privacy that are not addressed in the current European legal framework. Though the level of interference with the private sphere of the individuals might defer with the use of different devices (what can be learned from GPS devices about movements in the public space is certainly less intrusive than the personal information that can be learned from smart meters or smart phones), all the three case studies presented the possibility for incidental surveillance, mass surveillance and retroactive surveillance. Smartphones also showed the possibility that some devices might have for giving access to different categories of data at the same time.

The analyses contributed to a concrete assessment of the adequacy of the existing legal framework. Even though it is shown that different technologies might present additional challenges for the protection of the right to privacy of the individuals, two main ways for safeguarding the right are identified. The first one is technical and directed to the designers of devices and service providers. The second one is legal and directed to law enforcement and oversight authorities.

Designers of devices and service providers need to be more conscious of the surveillance capabilities of new technologies. It is important that they introduce the protection of the private sphere of individuals by design and default as an essential part of the products and services that they offer. For all the three cases discussed in this chapter, such a technical intervention would reduce the access of third parties to personal data and would limit State interferences to individual surveillance cases for which a specific surveillance warrant is required.

The new Data Protection Directive prescribes (in article 20) that by default only data which are necessary for the specific purpose of the processing are processed. Since according to its definition in article 3(2) processing explicitly covers also the collection of data, in a human rights' approach the outcome of this provision must be that non-purpose built devices, which for their design collect incidentally also other data, must not be used for surveillance.

In addition, since technology is advancing with very quick steps, specific laws are not the best and the speediest solution to the created problems. Instead of waiting for the legislator`s action, law enforcement and oversight authorities must rely on general rules of law and principles and use them in a protecting human rights lead approach to fill the existing or potential future gaps. The risks presented to the right to privacy and data protection of the individuals by the use for surveillance of non-purpose built devices must be assessed with the guidance of the principle of proportionality. The potential for incidental surveillance, mass surveillance, retroactive surveillance as well as the implications for the accuracy of the data must be evaluated in specific cases. This would give a more active role before the adoption of the surveillance measure to national authorities that issue surveillance mandates. At the same time, it will give more grounds for evaluating the proportionality of the decision *ex post*. The DPIA included in the new Data Protection Directive is not enough for this since it focuses only on data protection and is required for systems or processing operations that present high risks for the right of the individual, but not for specific cases. In the following chapter, the law enforcement access to information available via non-purpose built technology as well as the role of the proportionality principle and the operation of the structures of surveillance oversight are discussed in detail.

Chapter 5 Law enforcement access to information available via non-purpose built technology and the structures of surveillance oversight

5.1 Introduction

The legal framework that operates at European level and applies in cases of law enforcement surveillance of the private life of the individuals was discussed in chapter 3. The analyses showed that even though surveillance with non-purpose built technology and the challenges that it presents for safeguarding the right to privacy are not explicitly regulated, they are covered by the same legislation that regulates traditional surveillance and the proper use of some identified principles of law is a valuable asset for safeguarding the rights of the individuals. However, the conclusion that the level of safeguards that individuals have in cases of surveillance with non-purpose built technology is the same as in cases of traditional surveillance, does not mean that individuals have a proper protection of their private life in such situations. As it was already argued and confirmed by the case studies in chapter 4, the main problems that arise with the use of non-purpose built technology for surveillance are linked with incidental surveillance, mass surveillance and retroactive surveillance. In neither of these cases the current EU legislation and case law presents proper safeguards.

As the case studies showed, if non-purpose built devices are used for surveillance it is important to have an increased and specific care when law enforcement accesses the data and when surveillance authorizations are issued. Adding to the previous analyses, this chapter pays particular attention to these two elements - the access to the data by law enforcement and the structures of surveillance oversight. In this way, it further assesses if the right to privacy is properly protected by the current legal framework in situations of surveillance with non-purpose built technology.

Firstly, and addressing the third sub-research question, the chapter focuses on the law enforcement potential access to information collected via non-purpose built technology. This gives the possibility to evaluate the legality of law enforcement making use of the privately collected data. Non-purpose built devices used for surveillance are in the hands of individuals and the data that they collect is available first with service providers or other private parties.

Secondly, and addressing sub-research question four, it focuses on the ability of structures of surveillance oversight to properly assess the use of non-purpose built technology for law enforcement surveillance. The addressing of this issue gives the possibility to assess if the way

surveillance oversight operates, dictated by the traditional surveillance experience, is adequate also for cases of surveillance with non-purpose built technology.

After this very short introduction, section 5.2 focuses on the safeguards for the law enforcement potential access to information collected via non-purpose built technology. Special attention is devoted to situations in which law enforcement authorities collaborate with private parties that have access to the data. Section 5.3 focuses on the oversight structures for surveillance authorizations and assesses if national authorities have the necessary information required for adopting their decisions in cases of surveillance with non-purpose built technology. The section takes a fundamental rights approach and assesses the importance of the proportionality principle for adopting such decisions. In section 5.4 are summarized the main conclusions.

5.2 Law enforcement potential access to information collected via non-purpose built technology

The existing safeguards elaborated at EU and Council of Europe level tend to regulate the simultaneous existence of different, even though not necessarily conflicting, interests of the individuals and of the society. On one side, the rights of individuals for having their private life and personal data protected, and on the other side the interest of the society as well as of the individuals for national, public and personal security.

As already discussed in chapter 3 interference with the private life of individuals by State actors is allowed in the EU only in the presence of one of the listed situations (article 8(2) ECHR) and when it is provided by laws and in compliance with the principles of necessity and proportionality. Surveillance measures by law enforcement authorities qualify under the situations that allow the limitation of the right. The meaning of "provided by law" as well as the interpretation of the principles of necessity and proportionality by the European Court of Human Rights were already elaborated in chapter 3. These safeguards regulated in the basic laws aim to control any arbitrary behaviour by State actors and to protect the rights of the individuals.

Surveillance via the means of non-purpose built technology has to follow the same rules as other situations of surveillance, though the case studies of chapter 4 showed that the challenges presented to the right to privacy are not addressed. Law enforcement access to information available via these devices requires a mandate issued by competent authorities in the respect of the existing safeguards. Surveillance mandates must be reviewed by oversight structures (judicial or independent administrative bodies) whose decisions would seek to limit access to the data to what is strictly necessary.[738] The involvement of such oversight structures is to be considered in light of the proportionality principle and has the effect to limit the discretion of the law enforcement authorities. The use of non-purpose built technology for the scope of mass surveillance will require the explicit

[738] Joint Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 62

inclusion of these devices in mass surveillance programmes (as it was the case with the Data Retention Directive that regarded metadata collected via means of electronic communications).

Surveillance via non-purpose built technology has an effect also for the time of surveillance creating the possibility not only for access to the data on the spot, but also for data retention and the accessibility of these data at a different moment in time that is defined for this study as retroactive surveillance. For this situation the existence of procedural and substantive national rules on the storage as well as on the access to the data are required as a safeguard for the individuals.[739] Clear rules and objective requirements are required for the period of data retention.[740] The existing safeguards include also the irreversible destruction of the data[741] after the expiry of the retention period, the compliance with the principles of data minimization,[742] consent[743] and anonymization[744] as well as clear rules on the storage of the data.[745] The existing safeguards were seen, however, not to present a proper solution when other rights of the individuals, as for example the one to presumption of innocence, are interfered with by the retroactive surveillance.

As the example of retroactive surveillance shows and as it was already seen in chapter 2, surveillance with non-purpose built technology has an effect for the nature of the active subject of surveillance. It increases situations of horizontal surveillance, i.e. situations when surveillance is performed not directly by law enforcement authorities but from other private parties. In these situations, law enforcement authorities have the possibility to access the data directly via the used technologies or, in alternative, to obtain the data by the private parties, being these service providers or other private parties that have access to the data.

In case that the involvement of private parties in the surveillance activity would change the level of safeguards with which law enforcement authorities have to comply, such situations would severely diminish the protection of the fundamental rights of the individuals. In the following sub-sections is first discussed the qualification of surveillance via private parties in Europe. Subsequently it is assessed if the access that third parties have to the personal information of others due to the technology affects the level of safeguards required by law enforcement authorities. This assessment is done by making use of the principle of reasonable expectation of privacy.

[739] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 60
[740] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 64
[741] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 67
[742] This is in accordance with data minimization principle that derives from article 6(1)(b) and (c) of Directive 95/46/EC
[743] Data Protection Directive 95/46/EC, article 2(h)
[744] There are studies, however, that show an easy possibility for re-identification of smart meter data in 68,3% of the cases. See Buchman, E., Boehm, K., Burghardt, T., Kessler, S. (2013) Re-identification of smart meter data, *Personal and Ubiquitous Computing*, vol. 13, no.6, pp. 653-662
[745] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 60

5.2.1 State surveillance via private parties

Law enforcement authorities in their surveillance activities might involve private parties to collaborate and facilitate their work. These private parties can be natural or legal persons that for one reason or another have access to private data from individuals (as for example electricity service providers that notice abnormal changes in the electricity consumption of a household which might be linked with the engagement in illegal activities). The involvement of private parties can be voluntary or obligatory as it was the case under the (already discussed) Data Retention Directive or with the new the Anti-Money Laundering Directive.[746] However, as already stated, the involvement of private parties in the law enforcement activities must not circumvent the duties of the latter to act in accordance with all the legal safeguards.

In European law, legal entities (undertakings) which collaborate with the State and have for this reason special powers, qualify as an extension of the later.[747] As such they also have the same duties. In the *PNR* case the CJEU argued that despite the fact that passengers' data are collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, this should still fall under the provisions that regulate activities of the State or of State authorities.[748] It would thus be the essential objective or the final purpose for which data processing is undertaken the one to determine the applicable legal rules.

The ECtHR has used similar reasoning also for natural persons. Their activities qualify as State activities in those situations, for example, in which law enforcement authorities have not been involved directly in the interference with the private life of the individuals but have been receiving the needed information from other private parties.[749] Such situations are seen as falling under Article 8 ECHR and therefore qualify as State interference with the individuals private life.[750] This would be the case if, for example, a communication is intercepted by one of its parties, on its own initiative, while the law enforcement authorities, even though not directly involved, have been informed. For the ECtHR, the consent from one of the parties to the recording does not change the private character of a conversation.[751] In addition the ECtHR is aware that such practices might be

[746] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015, p. 73–117; Milaj, J., Kaiser, C. (2017) Retention of data in the new Anti-Money Laundering directive – 'need to know' versus 'nice to know', *International Data Privacy Law*, DOI:https://doi.org/10.1093/idpl/ipx002

[747] In general, on the qualification of private entities as emanations of the State for specific purposes see: Chalmers, D., Davies, G., Monti, G. (2014) European Union Law, 3rd edition, Cambridge, p. 312; case C-180/04 Vassallo v. Azienda Ospedaliera Ospedale San Martino di Genova e Cliniche Universitarie Convenzionate [2006] ECR I-7251, para. 26

[748] C-317/04 and C-318/04 Parliament v. Council [2006] ECR I-4721, para. 58

[749] M.M. v. The Netherlands, ECHR application no. 39339/98, 8 April 2003, para. 42; A. v. France, ECHR application no. 14838/89, 23 November 1993, para. 38-39

[750] M.M. v. The Netherlands, ECHR application no. 39339/98, 8 April 2003, para. 42; A. v. France, ECHR application no. 14838/89, 23 November 1993, paras. 38-39

[751] A. v. France, ECHR application no. 14838/89, 23 November 1993, para. 36

dangerously infringing the rights of individuals if the authorities have the possibility to evade legal obligations by making use of private agents.[752] Therefore these situations will fall under the prohibition of the first paragraph of article 8 ECHR. Thus far there are no ECtHR decisions dealing with legal entities that collaborate with law enforcement authorities. But there are no reasons to believe that in eventual future cases the outcome will be different than in cases of natural persons.

The development of technology and the access that legal entities have on individuals' information has already alerted international bodies as for example the Council of Europe or the United Nations. In the legal documents adopted by these bodies legal entities are expected to take the necessary steps to protect individuals against any abuses of human rights.[753] The European acts direct the attention to the application of international acts in the field, more specifically of UN Resolution 17/4[754] and of the Guiding principles on business and human rights.[755] These acts require and alert legal entities that are in possession of personal data not to allow any access by State actors for unlawful purposes.

The transferal of data from private parties to law enforcement authorities creates a situation in which data collected for (e.g.) commercial purposes are processed for criminal purposes. The change in the purpose of the processing of the data has to comply with the principle of purpose limitation. For De Busser (2009) such a change in the purpose is incompatible with the existing EU legislation on data protection since it lacks a functional equivalence and the foreseeability from the data subject.[756] Article 29 Working party, on the other side, reasons in its Opinion 2013/3 that the processing of the data for a different purpose might be exceptionally compatible with the laws. For this it is required that: (i) the new purpose is specific and all data quality requirements are satisfied, and (ii) a substantive compatibility assessment is done which takes into account the relationship between purposes, the context in which the data are collected and the reasonable expectations of the data subjects, the nature of the personal data and the impact that the further processing has for the data subject, and the safeguards.[757]

[752] Van Vondel v. The Netherlands, ECHR application no. 38258/03, 25 October 2007, para. 49

[753] See Resolution 2045(2015) of the Parliamentary Assembly of the Council of Europe on Mass Surveillance, 21.04.2015, para. 6; see also European Parliament (2015) Resolution of 12 March 2015 on the Annual Report on Human Rights and Democracy in the World 2013 and the European Union's policy on the matter; see also Council of Europe (2015) Declaration of the Committee of Ministers on ICANN, human rights and the rule of law, 3 June 2015, para. 5

[754] See Resolution 17/4 adopted by the Human Rights Council on Human rights and transnational corporations and other business enterprises, 6.7.2011, para. 4

[755] See Guiding principles on business and human rights – Implementing the United Nations "Protect, Respect and Remedy" framework, annexed to the Human Rights Council Report (A/HRC/17/31) and endorsed in Resolution 17/4

[756] De Busser, E. (2009) Data protection in EU and US criminal cooperation, Antwerp: Maklu, p. 68

[757] Article 29 Working Party (2013) Opinion 3/2013 on purpose limitation, 2 April 2013; see further for a change in opinion also De Busser, E. (2014) Privatization of information and the Data Protection Reform, in S. Gutwirth et al. (eds.), *Reloading data protection*, pp. 129-149

The possibility for law enforcement to have assistance or to access personal data that are available via private parties, does not therefore eliminate the requirements to have a valid mandate, for cases of individual surveillance, nor to act on the bases of well-established rules for cases of mass surveillance. The rights of the individuals must not be circumvented in such situations. However, that apart some case law from the European Court of Human Rights in cases of collaboration of private parties with the police, for legal entities the guidance comes from international acts that do not have a binding effect and cannot be challenged before courts.

As of 2018, with the implementation and enforcement of the Data protection reform the choice of the applicable legal instrument is clarified. In its opinion on the draft Data Protection Directive, Article 29 Working party argues that the processing of personal data for purposes different than the ones of the original collection should have their own legal basis and safeguards.[758] This concern is addressed in the new Data protection package which provides for the use of the Directive 2016/680 every time data are processed for the scope of law enforcement, independent from the legal nature of the processor. "*For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive*."[759]

In involving private parties in surveillance activities, law enforcement must consider also the way the data is collected from these parties. It would be absurd if the service providers have collected and retained unlawfully personal data from individuals for commercial purposes (for example without their consent) and are thus caught for such an activity from the provisions of Regulation 2016/679, but for the purpose of law enforcement the data collection is considered as legal (since no consent is needed for collecting the data for law enforcement purposes). In such situations, private parties must be under a dual obligation, the new Regulation and the new Directive. The protection of privacy under the human rights' approach would require law enforcement to assess the lawfulness of the collection of the data before accessing them. The new Data protection package does not provide for such situations.

The possibility of private parties for accessing the data might bring to a situation in which it is argued that the private sphere of the individuals is already compromised since personal data are not that

[758] Article 29 Working Party (2015) Opinion 3/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, 1 December 2015

[759] Directive 2016/680, recital 11

personal anymore because of being already shared with third parties. In the following sub-section is analysed if the level of safeguards set for protecting individuals from interferences with their private sphere is compromised in those cases in which personal data are already known or shared with other private parties. The analysis is based on the case law of the European Court of Human Rights and the principle of reasonable expectation of privacy.

5.2.2 The level of safeguards when personal information is not limited within the private sphere of the individuals

In chapter 3, it was argued that situations of surveillance with non-purpose built technology are not specifically regulated in European law. Despite the characteristics that distinguish this form of surveillance from traditional surveillance, the same general rules and safeguards as in other cases of surveillance apply.

Since in many situations of surveillance with non-purpose built technology the information is accessible by third parties, being these service providers or other parties that have access to the data on the basis of contractual relations or for other reasons, it is questionable if individuals have the same level of safeguards from State interferences as in cases in which the information is purely private. Schwartz (1995), in an article regarding personal information available for the public sector in the USA, argues that individuals that use technology which clearly has the effect of intruding into their privacy, both from private parties, as for example service providers, or by State authorities, via surveillance, do not have a reasonable expectation of privacy or have a reduced one.[760] One can argue that a similar reasoning can be used also for the EU. Furthermore, De Hert et al. (2009) argue that due to the development of technologies that might be used for surveillance, the reasonable expectation of privacy that the individual has turns into a reasonable expectation of being monitored.[761]

In assessing such dilemmas this sub-section focuses on the level of safeguards for individuals in those situations in which personal data are disclosed to third parties. In doing this it makes use of the principle of "reasonable expectation of privacy" as applied in Europe.[762] The level of safeguards required when accessing information from individuals that make use of non-purpose built technology might be affected by their expectation of privacy in concrete cases. The sub-section will first discuss the "reasonable expectation of privacy" as established by the European Court of Human Rights and will subsequently apply the principle to situations of surveillance with non-purpose built technology.

[760] Schwartz, P. (1995) Privacy and participation: Personal information and public sector regulation in the United States, *Iowa law Review*, vol. 80, pp. 553-618

[761] De Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., Gonzales Fuster, G. (2009) Legal safeguards for privacy and data protection in ambient intelligence, *Pers Ubiquit Comput*, vol. 13, pp. 435-444

[762] Newell, B.C. (2011) Rethinking Reasonable Expectations of Privacy in Online Social Networks, *Richmond Journal of Law and Technology*, vol. 17, no. 4, pp. 1-62

5.2.2.1 The reasonable expectation of privacy in the case law of the European Court of Human Rights

The "reasonable expectation of privacy" test has its origins in the US and the British case law.[763] In the 1967 in *Katz*, US Supreme Court judge John Marshall Harlan introduced a two steps test including: (i) a subjective expectation of privacy in certain situations, and (ii) an objective expectation linked with the recognition of the expectation from the society.[764] The European Court of Human Rights has also used the "reasonable expectation of privacy" principle in some of its decisions as one of the ways for establishing if an infringement of the right to privacy embedded in article 8 ECHR exists, even though it is never used as the only reason for this. There might be different and contrasting argumentations on how this principle applies in cases of intrusions to the right to privacy via non-purpose built technology.

For the ECtHR, the existence of a "reasonable expectation of privacy" helps to determine the establishment of a breach of the individual's right to privacy as established in the first paragraph of article 8 ECHR. It has to be noted here that this is independent of the objective test established under article 8 ECHR, as well as of a possible justification of the interference that might be established on the basis of the second paragraph of the article.[765] The reasonable expectation of privacy is to be seen as a subjective element, linked with the feelings and expectations of an individual.[766] The principle does not limit, however, the expectation to privacy of individuals for activities taking place in private premises but extends to activities that take place outside private homes, in public spaces.[767] Even public information is covered by the principle. In *Rotaru* for example, the ECtHR recognized that a right to privacy exists when a government agency systematically collects and stores personal information, even when this information is public.[768] In such situations is the systematic or permanent collection of the data that would turn the situation to fall under the privacy protection domain. Even though one might argue that when a person walks in a public street he would inevitably be subject to the eyes of other individuals and therefore not have any reasonable expectation of privacy for such an activity, the criteria of systematic or permanent collection of the data would determine the qualification of the situation.

The reasonable expectation of privacy that individuals have from other member of the society is seen as benefiting mainly those who are not engaged in any illegal activity. On the contrary, as the ECtHR stated in the *Lüdi* case, when an individual engages in an illegal activity that is punishable, he runs

[763] Gomez-Arostegui, H.T. (2005) Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations, *California Western International Law Journal*, vol. 35, no. 2, pp. 153-202
[764] Katz v. United States 389 U.S. 347 (1967)
[765] Halford v. The United Kingdom, ECHR application no. 20605/92, 25 June 1997, para. 45
[766] Gomez-Arostegui, H.T. (2005) Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations, *California Western International Law Journal*, vol. 35, no. 2, pp. 153-202
[767] P.G. and J.H. v. The United Kingdom, ECHR application no. 44787/98, 25 September 2001, para. 57
[768] Rotaru v. Romania, ECHR application no. 28341/95, 4 May 2000, para. 43

the risk to encounter law enforcement forces, in uniform or undercover, whose task will be to discover and expose the illegal activity.[769]

The use of technology for surveillance changes the situation even though the nature of the technology has not been treated in detail in the ECtHR's decision. An exception to the nature of the technology used for surveillance make two cases linked with surveillance and disclosure of information collected via CCTV cameras. In the first case (*Peck*) the ECtHR focused on the systematic and permanent storage of information collected via CCTV cameras during a footage in a public street. Even if in such a situation normally one cannot claim to have a reasonable expectation of privacy, the permanent and systematic collection and storage of the information qualified the situation to fall under the protection of private life rules.[770] In the second case (*Perry*) the ECtHR went further. In this later case, an individual was convicted of a series of armed robberies after being identified by witnesses from filmed images that were taken from the CCTV cameras of a police station. Even though the individual was in a place where one could expect to be subject to surveillance, the ECtHR reasoned that Mr. Perry could have not been reasonably expecting the use of technology for scopes beyond the normal foreseeability of their use – in the concrete case the use of CCTV cameras filming for identification purposes.[771] Such a reasoning brought the situation to fall under the "reasonable expectation of privacy" principle, and therefore under the protection of article 8 ECHR.

Even though both in *Perry* and in *Lüdi* the ECtHR had to deal with situations in which an individual was involved in illegal and punishable activities, the outcome of the decisions is different. It was the use of technology for surveillance and the foreseeability in the normal use of devices which justified the reasonable expectation of privacy in the *Perry* case even though the individual was engaged (similarly with the *Lüdi* case) in illegal activities.

In a later case, *Uzun*, the ECtHR clarifies and brings together the criteria on the basis of which activities taking place in public spaces fall under the protection of the right to privacy. Apart the use of technology for a scope that goes beyond what is foreseeable and the systematic or permanent storage of the data, the ECtHR adds here also situations in which there has been compilation of data on a particular individual, processing or use of personal data as well as their disclosure.[772]

As the result of this body of case law it can be concluded that even though because of the devices used individuals find their information shared with third parties this does not compromise their right to a protected private life from abusive State interferences. The implications that this has for cases of surveillance with non-purpose built technology are discussed in the following sub-section.

[769] Ludi v. Switzerlands, ECHR application no. 12433/86, 15 June 1992, para. 40
[770] Peck v. The United Kingdom, ECHR application no. 44647/98, 28 January 2003, para. 59
[771] Perry v. The United Kingdom, ECHR application no. 63737/00, 17 July 2003, para. 41
[772] Uzun v. Germany, ECHR application 35623/05, 2 September 2010, paras. 43-48

5.2.2.2 The reasonable expectation of privacy in cases of surveillance with non-purpose built technology

In the previous sub-section it was seen that the principle of "reasonable expectation of privacy" covers both situations in which an individual finds himself in a private space or in a public space. From the case law of the ECtHR it was seen that for a situation to fall under the privacy protection rules while taking place in public it is required a systematic or permanent storage of the data as well as their compilation, processing, use or disclosure. These elements would bring the otherwise public situation to fall under the realm of the privacy protection rules and therefore to have the same safeguards applicable as in other situations of interference with the right.

In this study it is submitted that the reasonable expectation of privacy principle must cover also cases in which an individual uses technology without a privacy protection but as an open space (as for example when using social media without any privacy filters).[773] In analogy with situations that take place in public spaces it can be argued that despite placing the data openly on the net the individual has an expectation of privacy in situations in which the data are systematically or permanently stored, compiled, processed, used or disclosed. This reasoning brings such situations fall under the privacy protection rules and therefore requires from the authorities to follow the same safeguards as when surveilling other private activities of the individual. It was already argued in this chapter that the involvement of private parties in surveillance activities does not lower the safeguards that State authorities must follow when accessing the data.

The nature of the technology used for surveillance is also relevant for having a reasonable expectation of privacy. It was seen that the foreseeability of the expected use of technology is one of the criteria for turning a, otherwise not protected, situation as falling under the privacy protection rules. In case of surveillance with non-purpose built technology it is clear that the technology is used in ways beyond its normal purpose. The use of the technology in such cases, beyond its normal use, is not foreseeable to the individual. This would bring such situations into the realm of the privacy protection rules. In addition, as already seen in *Perry* and in *Uzun*, the involvement of the individual in illegal activities does not influence his reasonable expectation of privacy when the interference with the right is the result of the non-foreseeability in the use of a device beyond its normal function. For national authorities there is as a result an obligation to use at least the same level of safeguards as in other cases in which they interfere with the private sphere of the individual.

5.2.3 Concluding remarks

This section discussed the potential access of law enforcement in information that is collected with devices that are not built for the purpose of surveillance. It was argued that in those cases in which

[773] See also Koops, B.-J. (2013), Police investigations in Internet open sources: procedural-law issues, *Computer Law & Security Review*, vol. 29, n. 6, pp. 654-665

there is an interference with the rights of privacy and data protection of the individuals the general safeguards established at European level in the legal rules and jurisprudence apply.

The general safeguards apply also for the cases of access to information collected with non-purpose built technology independent of the fact that State authorities access the information directly or via third parties that have access to the same information. The fact that individuals use technologies that are more prone to surveillance and interferences with their private lives by State authorities or other private parties is not changing the level of safeguards that protects them in such situations. This conclusion is a logical consequence of the case law of the European Court of Human Rights on the reasonable expectation of privacy.

Bringing situations that take place in public spaces into the realm of privacy protection opens the doors for protection of individuals also in those cases in which they jeopardize their privacy by not setting proper privacy protection filters for their activities. In addition, the use of non-purpose built technology for surveillance scopes is similar with situations in which a person is not reasonably expected to foresee the use of technology beyond its normal use. Such situations belong to the realm of privacy protection and must benefit from, at least, the same safeguards designed for the protection of privacy and personal data in general.

5.3 The law enforcement structures of surveillance oversight and the role of the proportionality principle as a general safeguard

After discussing the access to information collected via non-purpose built technology and arguing that the same safeguards for the individuals apply as in other cases of surveillance, this section focuses on the surveillance authorization and the law enforcement structures of surveillance oversight. The law enforcement structures of surveillance oversight for this study cover the State bodies authorized for issuing surveillance mandates and their follow-up supervision. These structures tend to be persons, or bodies that are not engaged in the day to day conducting of the investigation. Usually they are identified as judicial bodies, but in some States decisions are taken also by prosecutors, authorized police authorities or administrative bodies as in the case of a government minister.

Oversight structures are seen as the means for ensuring the accountability of decisions of authorities.[774] Theoretically, such structures aim not only at avoiding the abuse of power by legitimizing it, but also to achieve better results in specific situations. With regards to intelligence

[774] Leigh, I. (2005) More closely watching the spies: Three decades of experiences, at Born, H. et al. (eds.) *Who's watching the spies?: Establishing intelligence service accountability*, Potomac Books, Washington, pp. 3-11

services, for example, it is argued that the oversight should be a combination of executive control, parliamentary oversight, judicial review and expert bodies.[775]

With regards to law enforcement oversight, both the Court of Justice of the EU[776] and the European Court of Human Rights argue for the need of independent oversight structures of judicial or administrative nature. In *Popescu*[777] the ECtHR considered that the military public prosecutor that ordered the surveillance measure in the concrete case was not to be considered as independent from the executive branch. It further stated that the authorizing body must be independent and that there should be either judicial or independent control over its activity.

In the *Iordachi*[778] and *Ekimdzhiev*[779] cases the ECtHR stressed that independent controls should exist both at the authorization as well as at the oversight fase. From the case law it looks as if the ECtHR has a preference for judicial authorization, even though in *Kennedy*[780] (regarding intelligence services) it argued in favour of the British system of government authorization.

In the words of the Council of Europe Commissioner for Human Rights, "*It is individual members of security services that play the most significant role in ensuring that security service activity is human rights compliant and accountable. External oversight can achieve little if the security services do not have an internal culture and members of stuff that respect human rights*."[781] In this light the section will not discuss further the nature of national oversight structures. Other studies have already done it.[782] The specific focus of this section is on the importance of the proportionality principle that must guide these oversight authorities, independent of their nature, in adopting their decisions in conformity with the fundamental right to privacy.

[775] European Commission for Democracy through Law, Report on the democratic oversight of the security services, study no. 388/2006

[776] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 62

[777] Popescu v. Romania (no. 2), ECHR application no. 71525/01, 26 April 2007, paras. 70-73

[778] Iordachi and others v. Moldova, ECHR application no. 25198/02, 24 September 2009, para. 40

[779] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, ECHR application no. 62540/00, 28 June 2007, para. 89

[780] Kennedy v. the United Kingdom, ECHR application no. 26839/05, 18 May 2010, para. 166

[781] Council of Europe Commissioner for HR (2015), Democratic and effective oversight of national security services, issue paper

[782] See for example den Boer, M., Fernhout, R. (2008) Police oversight mechanisms in Europe: Towards a comparative overview of Ombudsmen and their competences, available online at: http://www.asef.org/images/docs/1270-Police_Oversight_Mechanisms_in_Europe.pdf (last check 12.1.2016); Gutwirth, S., De Hert, P. (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in Claes, E., Duff, A., Gutwirth, S. (eds.), *Privacy and the Criminal Law*, pp. 61–104; Coudert, F. (2014) Accountable Surveillance Practices: Is the EU Moving in the Right Direction?, in Preneel, B., Ikonomou, D. (eds.), *Privacy technologies and policy*, pp. 70-85

The analyses takes a fundamental rights approach to assess the information that oversight structures need for the proper use of the proportionality principle when deciding on surveillance measures that imply the use of technology, especially if this technology is not originally designed for the purpose of surveillance. As it was seen above, while the European legislator focuses on the protection of personal data, for the right to privacy the proper use of the principle of proportionality is the one to guide the safeguarding of the right. The section does not deal with the *ex post* complaint mechanisms, as for example legal review of surveillance decisions by national courts but with the way these decisions are taken and checked *ex ante*. Since technical sophistication makes it difficult for oversight surveillance structures to take their decisions without technical aid, the section will briefly review existing methods for privacy assessment of devices and will assess if national oversight structures are able to find in these methods the needed information for adopting their decisions.

After this introduction, sub-section 5.3.1 addresses the importance of the proportionality principle as a safeguard when limiting a fundamental right and especially the right to privacy. The principle is examined in light of the rules and especially of the case law in the Council of Europe (sub-section 5.3.1.1) as well as in the European Union (sub-section 5.3.1.2) framework. In sub-section 5.3.2 the information that national oversight authorities need for taking decisions in conformity with the proportionality principle is discussed. Sub-section 5.3.3 analyses different methods of assessing privacy and surveillance implications of technologies and devices and emphasises why the needed information cannot be found in them. Attention is paid in particular to the prior checking method and the data protection impact assessment in the EU (sub-section 5.3.3.1), the privacy impact assessment (sub-section 5.3.3.2), the surveillance impact assessment (sub-section 5.3.3.3), and the model for assessing the privacy 'cost' of a surveillance system proposed by Thommesen and Andersen (2009) (sub-section 5.3.3.4). Sub-section 5.3.4 presents a fundamental rights approach to the analysed methods of assessment. Sub-section 5.3.5 highlights the main findings and concludes.

5.3.1 The proportionality principle

The proportionality principle occupies a central place in this sub-section since it is the one to strike a balance between the fundamental right for a protected private life of the individuals and the societal interests for national security, public safety, prevention of disorder or crime, etc. Proportionality is the principle that must guide decisions of national authorities which interfere with the fundamental right to privacy.

Barak (2012) defines proportionality as the set of rules that determines the necessary and sufficient conditions for limiting a protected right.[783] Jans (2007) defines it as a principle that restricts the exercise of governmental powers.[784] In this light it can be said that the principle fulfils a dual role: it protects fundamental rights while providing at the same time a justification for their limitation.

[783] Barak, A. (2012), Proportionality – Constitutional Rights and their limitations, Cambridge University Press, p. 3

[784] Jans, J.H., et al. (2007), Europeanisation of Public Law, Europa Law Publishing, p. 143

In the presence of the need to limit a fundamental right, the proportionality principle is of particular importance. According to Harbo (2010), the principle can serve as an instrument for balancing conflicting interests in a way that does not give precedence to any of them. There are however no rationale standards for establishing a balance between two interests of the same level, and the weighting of interests can be sometimes arbitrary or unreflective, according to customary standards or hierarchies.[785]

Regarding interferences with fundamental rights, it is important that national authorities adopt proportionate decisions *ex ante* since the *ex post* complaint mechanism will not always be effective for various reasons. Firstly, an *ex post* evaluation of decisions on limiting fundamental rights can be complicated by the separation of powers and competences, i.e.: "*who should decide whether it [proportionality] has been observed or not?*".[786] The answer to this question becomes more complicated if we bear in mind that the proportionality principle does not have a normative value as such, and often national authorities have a margin of discretion in deciding. Secondly, another risk that arises in the context of an *ex post* evaluation of proportionality is that the balance might tilt towards accepting more intrusive measures in the face of more grave offences (as it was the case after the September 11 events, for example). In its evaluation proportionality is, after all, a flexible tool which applies differently in different contexts.[787] Thirdly, because of existing information asymmetries, it is difficult for national authorities to authorize the least intrusive surveillance measures available. The lack of information bringing to potentially wrong and disproportionate decisions might be justified in those cases by the flexibility characteristic that the proportionality principle has. Apart the authorities themselves, the information asymmetry affects also the individuals. They are not always informed on all the surveillance measures and especially techniques that were employed in their case. This lack of information would make a potential *ex post* complaint from their behalf quite unlikely.

These concerns highlight the need for a clear guidance for national oversight authorities to aid the proper and well informed use of the proportionality principle *ex ante*, i.e. when permitting the use of a device or technology for surveillance purposes. Even if it cannot be assured that decisions of these authorities will be proportionate, it is important to offer them the necessary tools and information to be able to take proportionate decisions.

[785] Harbo, T. (2010), The function of the proportionality principle in EU law, in *European Law Journal*, vol. 16, no. 2, pp. 158-185

[786] Hoffmann, L. (1999), The influence of the European principle of proportionality upon UK law, in Ellis, E. eds., *The principle of proportionality in the laws of Europe,* pp. 107-115

[787] Jacobs, F.G. (1999), Recent development in the proportionality principle in European Community law, in Ellis, E. eds., *The principle of proportionality in the laws of Europe,* pp. 1-21

For a good understanding of the proportionality principle and its role in balancing conflicting interests, it is important to understand how the principle is being interpreted by the courts.[788] In the following sub-section is discussed the development of the principle first in the context of the Council of Europe and then in the context of the European Union.

5.3.1.1 Development of proportionality in a Council of Europe context

The proportionality principle as such is not explicitly mentioned in the European Convention of Human Rights, but according to the European Court of Human Rights rulings it is a central feature of human rights.[789] In this framework, the principle is also used for establishing a balance between the right to a 'protected private life of the individuals' and 'the interest for a safer society and protection of national interests'.[790] In order not to restrict the rights of the individuals unnecessarily in return for societal benefits, Arai-Takahashi (2002) argues that a delicate balance must be struck between the employed means and the pursued scope.[791] Following this logic, it is necessary for authorities to decide upon the appropriate surveillance measures and means on a case by case basis. Interference with the private sphere of the individuals are allowed only in those situations where there are no other means to safeguard the higher societal interests in a way that is less intrusive and less restricting the rights of the individuals.[792]

According to Eissen (1993), the ECtHR first used the proportionality principle in the *Handyside* decision.[793] In this case the ECtHR presented a strict approach for the limitation of a fundamental right that can be brought down to the following four questions´ test: (i) Is there the presence of a pressing social need for restricting the rights of the Convention? (ii) Does the particular restriction correspond to this need? (iii) Is the restriction a proportionate response to that need? (iv) Are the reasons presented by the authorities, relevant and sufficient?[794]

[788] Taylor, N. (2011), A conceptual legal framework for privacy, accountability and transparency in visual surveillance systems, *Surveillance and Society*, vol. 8, no. 4, pp. 455-470; according to this author the proportionality principle plays a role in establishing a balance between the nature and the extend of the interference against the reasons for interfering

[789] McBride, J. (1999), Proportionality and the European Court of Human Rights, in Ellis, E. eds., *The principle of proportionality in the laws of Europe*, pp. 23-36; Sunday Times v. The United Kingdom, ECHR application no. 6538/74, 26 April 1979, para. 13

[790] Taylor, N. (2003), Policing, privacy and proportionality, *European Human Rights Law Review, Supplement (Special issue: Privacy 2003)*, pp. 86-100

[791] Arai-Takahashi, Y. (2002), The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR, Intersentia, p. 14

[792] De Hert, P. (2005), Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, vol. 1, no. 1, pp. 68-96

[793] Eissen, M. (1993), The proportionality principle in the case law of the European court of Human Rights, in Macdonald, R.St.J., Matscher, F. and Petzold, H., eds., *The European System for the Protection of Human Rights*, pp. 125-137

[794] Handyside v. The United Kingdom, ECHR application no. 5493/72, 7 December 1976, para. 49

In other cases the ECtHR employed more abstract language, referring to proportionality as "*a reasonable relationship between the means and the aim sought to be realised*" or "*a fair balance*" between the general and individual interests at stake.[795] In addition, interferences are considered to be disproportionate if they impair the very essence of the right,[796] as well as in situations in which the State has not made all the necessary positive arrangements to guarantee the effectiveness of the protection of the right.[797]

From the above elaboration of the case law it is clear that, even if not codified at Council of Europe level, the proportionality principle is the one that is assessed when evaluating decisions of national authorities to limit a fundamental right. According to some authors, however, the ECtHR has been quite keen in applying the principle and in giving a clear explanation of it. The reason brought forward for this is to be found in the intrinsic complexity of the principle itself.[798] This is related also with the fact that the ECtHR respects the margin of discretion enjoyed by national courts and recognizes that the exclusivity to interpret and apply national law to domestic situations should remain within the domain of national authorities.[799] This approach becomes even stronger in cases where measures are introduced with the scope of protecting national interests. In such situations, the ECtHR reiterated on several occasions that it is for the national authorities to judge what is necessary and proportionate in order to protect the domestic interests. The attention of the ECtHR in such cases is focused on the analyses of the legal safeguards and guaranties offered to the individuals.[800] This is also related, of course, with the separation of powers. The ECtHR takes only a marginal view of the application of the principle when national authorities have a margin of discretion to decide.[801] It is difficult for the courts at national or international level to evaluate decisions taken by national authorities to which the legislator, apart the competence for deciding, has left also a margin of discretion. This does not mean, however, that national authorities can adopt their decisions in violation of the proportionality principle or that they might disregard the principle when adopting their decisions.

The obligation of the State and of national authorities is not limited to a negative obligation not to interfere with the life of the individuals, but is extended to a positive obligation, requiring the State to effectively and inherently insure the protection of their private sphere.[802] If the State does not take all the necessary steps to protect the private sphere of the individuals in horizontal situations,

[795] Peck v. The United Kingdom, ECHR application no. 44647/98, 28 January 2003, para. 70
[796] Rees v. The United Kingdom, ECHR application no. 9532/81, 17 October 1986, para. 50
[797] Marckx v. Belgium, ECHR application no. 6833/74, 13 June 1979, para. 31; Gaskin v. The United Kingdom, ECHR application no. 10454/83, 7 July 1989, paras. 42-49
[798] De Hert, P. (2012), A human rights perspective on privacy and data protection impact assessment, in Wright and De Hert eds., *Privacy Impact Assessment*, Springer, pp. 33-76
[799] Arai-Takahashi, Y. (2002), The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR, Intersentia, p. 14; Kruslin v. France, ECHR application no. 11801/85, 24 April 1990, para. 29
[800] Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006, para. 106; Klass v. Germany, ECHR application no. 5029/71, 6 September 1978; para. 50
[801] Jans, J.H., et al. (2007), Europeanisation of Public Law, Europa Law Publishing, p. 151
[802] Marckx v. Belgium, ECHR application no. 6833/74, 13 June 1979, para. 31

when other private parties interfere with the rights, the disproportionality of the situation is debited to the State and falls under the protection of article 8(1) ECHR.[803] Positive measures are required to be taken in such situations regarding the sphere of relations between individuals.[804]

Having adequate guarantees against abuse by public authorities is a way to secure the protection of the rights of individuals.[805] However, it is clearly more desirable to prevent than to cure. As suggested above, proportionality would be an important guidance for oversight structures at the moment that they evaluate and authorize the use of a surveillance measure, and serve therefore better as an *ex ante* rather than an *ex post* safeguarding tool.

5.3.1.2 Development of proportionality in a European Union context

At European Union level the proportionality principle is codified in article 52(1) of the Charter of Fundamental Rights which constitutes a condition to be fulfilled when a necessity (a need) requires the limitation of non-absolute rights.[806] The principle was, however, fully developed beforehand by the European Court of Justice in the 1970s in the case *Internationale Handelsgesellschaft.*[807]

Akin to the German administrative law, at EU level the test for establishing the proportionality of a measure is composed of three steps: (i) appropriateness; (ii) necessity; and (iii) proportionality *stricto sensu*.[808] Any measure restricting fundamental rights must be first of all appropriate or suitable to protect the interests that require protection. It must be necessary, meaning that no measure less restrictive must be available to attain the objective pursued. And it must be proportionate *stricto sensu*, meaning that the restriction that it causes must not be disproportionate to the intended objective or result to be achieved.[809] The CJEU does not always distinguish, however, between the second and the third step of the test, the necessity and the proportionality *stricto sensu* of a measure.[810]

---

[803] Marckx v. Belgium, ECHR application no. 6833/74, 13 June 1979, para. 31; X & Y v. The Netherlands, ECHR application no. 8978/80, 26 March 1985, para. 23; Gaskin v. The United Kingdom, ECHR application no. 10454/83, 7 July 1989, paras. 42-49

[804] Eissen, M. (1993), The proportionality principle in the case law of the European court of Human Rights, in Macdonald, R.St.J., Matscher, F. and Petzold, H., eds., *The European System for the Protection of Human Rights*, pp. 125-137

[805] Malone v. The United Kingdom, ECHR application no. 8691/79, 2 August 1984, para. 81

[806] The proportionality principle is central also in the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, Official Journal L 350, 30/12/2008, see for example Article 3

[807] Barak, A. (2012), Proportionality – Constitutional Rights and their limitations, Cambridge University Press, p. 185

[808] Troncoso Reigada, A. (2012), The principle of proportionality and the fundamental right to personal data protection: The biometric data processing, *Lex Electronica*, vol. 17, no. 2, pp. 1-44

[809] Jans, J.H., et al. (2007), Europeanisation of Public Law, Europa Law Publishing, p. 149

[810] C-159/90 The Protection of Unborn Children Ireland Ltd v. Stephen Grogan and others, [1991] ECR I-04685, Opinion of AG van Gerven, para. 27; for a clarification of the necessity and proportionality stricto sensu steps of the proportionality test see Rivers, J. (2002) A theory of Constitutional rights and the British Constitution, A

As a general principle of law, proportionality has been developed by the CJEU primarily with a view of protecting the individual from interference by Union institutions or by Member States. It requires the reaching of a proper balance between the individual's interest and the desired general interests.[811] The proportionality principle as applied by the European Court contains a very strong substantial bias.[812] This is reflected in the different way the CJEU uses the principle when assessing EU or national measures.

When challenging the validity of EU law, the CJEU assesses if the measure is manifestly inappropriate. The Court is called upon to balance a private against a public interest. The underlying interests which the principle seeks to protect are the rights of the individual but, given the discretion of the European legislator, the review of the policy measure is based on the so-called 'manifestly inappropriate' test.

On the other side, when challenging the validity of a national act, the CJEU applies a stricter test and examines if it would have been possible for the Member State to adopt a less restrictive alternative.[813] In this case the CJEU is called upon to balance a Union interest against a national interest. The proportionality principle is applied as a market integration mechanism and the intensity of review is much stronger. It is based on necessity[814] exemplified by the '*less restrictive alternative*' test.[815] The alternative method is not required, however, to be the most effective or practical solution. This view is supported also by Jacobs (1999) that considers the existing dichotomy as having

translator's introduction in Alexy, R. A theory of constitutional rights, OUP, p. xxxi: "*Necessity asks whether any less intrusive means would achieve the same end, which is essentially an empirical question of prognosis and causation, and proportionality asks whether the end is worth pursuing, given what it necessary costs. It is important to see that necessity and proportionality (in the narrow sense) are different tests: a measure may be the least intrusive means to achieve a certain end, and yet even the least intrusion necessary may be too high a price to pay in terms of the interference with other legally recognized interests*."

[811] Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [2010] ECR I-11063, para. 86; Mifsud Bonnici, J.P. (2013), Exploring the non-absolute nature of the right to data protection, *International Review of Law, Computer and Technology*, vol. 28, no. 2, pp. 131-143

[812] Tridimas, T. (1999), Proportionality in European Community law: Searching for the appropriate standard of scrutiny, in Ellis, E. eds., *The principle of proportionality in the laws of Europe*, pp. 65-84; C-84/94 United Kingdom v. Council [1996] ECR I-5755, para. 57; C-265/87 Schraeder HS Kraftfutter GmbH & Co KG v. Hauptzollamt Gronau [1989] ECR 2237; paras. 21-27

[813] See Case C-524/06 Heinz Huber v. Bundesrepublik Deutschland [2008] ECR I-09705, Opinion of AG Maduro, para. 16

[814] Galetta, A., De Hert, P. (2014) Complementing the surveillance law principles of the Court of Strasbourg with its environmental law principles. An integrated technology approach to a human rights framework for surveillance, *Utrecht Law Review*, vol.10, n. 1, pp. 55 – 75; Greer, S. (1997) The exceptions to Articles 8 to 11 of the European Convention of Human Rights, *Human Rights Files*, no. 15, pp. 14-15, Council of Europe Publishing

[815] Tridimas, T. (1999), Proportionality in European Community law: Searching for the appropriate standard of scrutiny, in Ellis, E. eds., *The principle of proportionality in the laws of Europe*, pp. 65-84

good reasons. The scrutiny of national measures may need to be more demanding where these are likely to impair the effectiveness of Union measures.[816]

Leaving aside any policy reasons mentioned above, the approach of the CJEU leaves individuals less protected in the presence of EU measures since the proportionality principle is not used for choosing between possible alternatives. The reluctance of the CJEU to use the '*less restrictive alternative*' test when judging Union measures was clearly seen in the invalidation of the Data Retention Directive case[817] where the necessity step of the proportionality test was reduced to a '*limited to what it is strictly necessary*' analyses.[818] Despite these incongruences, it is clear that also at European Union level the proportionality principle is seen as the one to be used by national as well as Union authorities and oversight structures when deciding on the limitation of a fundamental right.

5.3.2 A proportionate decision

From the interpretation that the courts at Council of Europe and European Union level give to the principle of proportionality, even though the test they follow is similar and thus should bring at consistent outcomes, it is clear that because of political reasons the protection of the principle is not satisfying. At the ECtHR level, this is due to the margin of appreciation left to the national courts and at the CJEU level, is due to the difference in treating national or European decisions. When dealing with restriction of human rights it would thus be preferable to address proportionality before taking a decision rather than *ex post*.

In the beginning of this section it was argued that surveillance oversight structures require information that enables them to authorize proportionate surveillance measures. Since surveillance implies more and more the use of technology and of devices not designed for that purpose, the authorities need information on the technologies they seek to employ in order to enable them to take decisions in conformity with the fundamental right to a protected private life and the principle of proportionality. This sub-section will give a brief overview of this required information.

The information national authorities currently have on technical devices is limited. For this reason De Hert (2005) suggests that a formal approach towards the legality requirement – "*no* [use of] *technology without law*" – would be more in line with the constitutional wisdom.[819] This suggestion derives from the awareness that it is difficult to expect that the assessment of the compatibility of technology with the protection of the individuals´ private life will be properly done by national

[816] Jacobs, F.G. (1999), Recent development in the proportionality principle in European Community law, in Ellis, E. eds., *The principle of proportionality in the laws of Europe,* pp. 1-21

[817] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 52

[818] Milaj, J. (2015) Invalidation of the Data Retention Directive – Extending the proportionality test, *The Computer Law and Security Review*, vol. 31, no. 5

[819] De Hert, P. (2005), Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, vol. 1, no. 1, pp. 68-96

authorities in the absence of clear and specific rules. As a result, De Hert suggests that it is better if national authorities will be able to authorise only the use of those methods of surveillance and devices for which it is explicitly provided in the laws. However, it is quite impossible and improbable for legislation to keep the same speed with the technology that develops by the minute. This has created at the moment a regulatory disconnection between the legal framework and technology. For mitigating this gap, a clear roadmap for the privacy implications of devices that might be used for surveillance is needed. This roadmap will aid national authorities in taking their decisions independent of their (sometimes technology-lacking) background.

As already seen, technological development has created the possibility for many devices to be used for the scope of surveillance, independent of their original purpose.[820] As the example of location tracing shows, there is more than one device that might be able to provide the same information. The way these devices interfere with the private life of the individual might, however, differ. While the data collected from a GPS device will give information on the geo location of an individual or vehicle in open spaces, a smart phone (that is normally carried close to the body in a pocket or bag) might give more accurate location information including also private spaces. Apart disclosing the location, a smart phone might be used also for intercepting communications, as a portable bug,[821] for identifying the online behaviour of an individual, etc. Both devices might also collect incidentally information from third parties that make use of these devices.[822] The surveillance authorisation that a national authority will issue must therefore be proportionate to the identified needs of a specific case and minimize the other possibilities for interfering with the private life of the individuals.

The first information that national authorities must have for taking their decisions are the alternative devices that might be employed for reaching the same result. The choice of a device to be used in a specific case must be done after an assessment of the possibilities they offer to interfere with the private life of the individuals. For this attention must be paid on one side to all aspects of privacy and on the other to the dimensions of surveillance. The interference of devices with any of these aspects of the private life that are identified thus far[823] must be taken into account when deciding on its use for surveillance.

Apart identifying the aspects of the private sphere of the individual that are being intruded, it is important to evaluate also the level of intrusiveness of the method of surveillance and the devices

[820] Mobbs, P. (2003), Privacy and Surveillance: How and when organisations and the state can monitor your actions, *GreenNet CSIR*, no. 3, available online at: http://www.internetrights.org.uk/briefings/irtb05-rev1-draft.pdf (last accessed: 17.6.2015)

[821] McCullagh, D., Broache, A. (2006), FBI taps cell phone mic as eavesdropping tool, *CNet News*, available online at: http://news.cnet.com/2100-1029-6140191.html (last accessed: 16.6.2015)

[822] "Collateral intrusion" is defined in the UK in a guiding document to the application of RIPA as interference with the privacy of persons, other than the subject of the surveillance.

[823] Clarke, R. (2006), What's 'Privacy'?, available online at: http://www.rogerclarke.com/DV/Privacy.html (last accessed: 17.6.2015); Wright, D., Raab, C.D. (2014), Privacy principles, risks and harms, *International Review of Law, Computers and Technology*, vol. 28, no. 3, pp. 277-298

that can be used. For this evaluation, the dimensions of surveillance need to be assessed. As already seen in chapter 2, Marx (2002) has identified 26 dimensions of surveillance starting with the way the senses are aided by the devices, to the possibilities for analysing, merging and communicating the information.[824] The level of intrusiveness into the private life of the targeted individuals as well as the potential intrusion into the private life of third parties must be carefully assessed by the authorities that decide upon the surveillance measure.

The knowledge of the aspects of privacy interfered with, the level of interference and the interference with the lives of third parties will give national authorities the possibility to take an informed decision which complies with the fundamental rights of the individuals as well as with the principle of proportionality. The assessment will guide authorities to select and authorise the use of the less intrusive surveillance method and device. This evaluation is independent of what is the most practical or effective solution in a specific case. Interferences with the private sphere of the individuals will be considered as proportionate in those situations in which the prevailing societal interest that requires the interference cannot be safeguarded with measures which are less intrusive and less restricting the rights of the individuals.[825]

5.3.3 Privacy assessment methods

This sub-section focuses on existing methods for assessing privacy implications of devices and analyses why national oversight authorities cannot find in them the information they need for adopting proportionate surveillance authorisations.[826] As already discussed earlier, national surveillance oversight structures are the ones responsible to decide upon the use of a particular surveillance method and device. These structures have the duty to refrain from any potential abuse of their authorisation since the private sphere of the individuals is protected as a fundamental right in the European Union.

At their start, impact assessment methods for identifying potential privacy or data breaches were not backed up by a legal obligation.[827] They have been designed as recommendations or even good practices and were mainly targeting technology designers and the private sector with the aim to increase their awareness and introduce protection of the private life of the citizens as one of the

[824] Marx, G. (2002), What is new about "New surveillance"? Classifying for change and continuity, *Surveillance and Society*, vol. 1, no. 1, pp. 9-29

[825] De Hert, P. (2005), Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, vol. 1, no. 1, pp. 68-96

[826] Part of this research is already published in: Milaj, J. (2015) Privacy, surveillance and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance, *International Review of Law, Computers and Technology*, DOI: 10.1080/13600869.2015.1076993

[827] Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M. (2016) A Process for Data Protection Impact Assessment under the European General Data Protection Regulation, in Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (Eds.) *Privacy technologies and policy*, pp. 21-37

characteristics of their devices.[828] From a parsimony and efficiency point of view it is desirable, however, to be able to use the existing methods for providing the needed information to national authorities before proposing to design a new one.

After discussing the prior checking and data protection impact assessment (sub-section 5.3.3.1) in the framework of the European Union the section discusses other methods that are being discussed for introduction in the EU such as: the privacy impact assessment method (sub-section 5.3.3.2), the surveillance impact assessment method (sub-section 5.3.3.3) and, a model proposed by Thommesen and Andersen (2009)[829] for assessing the privacy 'cost' of a surveillance system (sub-section 5.3.3.4). Privacy auditing and compliance reviews[830] are not considered since they have a narrow focus on the compliance with applicable privacy laws, regulations or other rules to which a data user is subject.[831] Their scope is to present a legality check of a device. These methods, consequently, do not pay attention to technical features of devices which impact the privacy of individuals.

5.3.3.1 Prior checking in the EU and the data protection impact assessment

As already seen, security and surveillance related matters lack a common regulatory framework in the European Union.[832] Furthermore, regarding the rights to privacy and data protection the focus of the EU secondary legislation thus far weights largely on data protection and not on privacy. This limited approach of the European legislator leaves most of the aspects of the private sphere of the individuals uncovered and is considered as regressive by Wright and Raab (2014).[833] It looks almost as if the legislator wrongly believes that regulating data protection issues would by itself solve also the problems faced by the right to privacy. The absence of secondary legislation related with privacy issues directs the attention to data protection rules.

[828] ICO (2014) Conducting privacy impact assessments code of practice, available online at: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (last accessed: 27.10.2016); CNIL (2015) Privacy Impact Assessment: Methodology (how to carry out a PIA), available online at: http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf (last accessed: 27.10.2016)

[829] Thommesen, J., Andersen, H.B. (2009), Privacy implications of surveillance systems, available online at: http://orbit.dtu.dk/fedora/objects/orbit:56150/datastreams/file_4010841/content (last accessed: 6.5.2013)

[830] De Hert, P. (2012), A human rights perspective on privacy and data protection impact assessment, in Wright and De Hert eds., *Privacy Impact Assessment*, Springer, pp. 33-76

[831] Waters, N. (2012), Privacy impact assessment – Great potential not often realized, in Wright and De Hert eds., Privacy Impact Assessment, pp. 149-160

[832] The lack of a common framework does not mean however that sector specific laws dealing also with, privacy and surveillance, have not been adopted. See for example the Schengen agreements, creation of Europol and Eurojust, etc.

[833] Wright, D., Raab, C.D. (2014), Privacy principles, risks and harms, *International Review of Law, Computers and Technology*, vol. 28, no. 3, pp. 277-298

Article 20 of the Data Protection Directive[834] provides for a prior checking examination. This method provides that Member States shall determine processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined before the starting of the operation of the device. Prior checking serves to determine if processing of personal data will be done in compliance with the laws, or whether the system needs to be improved from a data protection perspective. Almost all the Member States have been implementing the provision in their national legislation. The operations that would fall under this provision, however, differ in the Member States. Prior checking is limited to sensitive data in Estonia and Greece, to certain risks in the Czech Republic, Ireland, Italy, the UK and Malta, and to certain cases in Lithuania.[835] The scope of the application of prior checking is not extended, however, to law enforcement activities.

The new Data Protection Regulation will substitute the existing Data Protection Directive as of 25th of May 2018. In article 35 it provides for a data protection impact assessment (DPIA): "*where those processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*" which would substitute the current prior checking examination. A DPIA is included also in article 27 of the new Data Protection Directive which involves the work of police and law enforcement for the prevention, detection, investigation and prosecution of crime. The new laws introduce the DPIA as a legal obligation to be carried out by data controllers, but it is of course still early to evaluate the way it will operate.[836] There are already voices against it. For De Hert (2012)[837] it would not be more than a compliance check while for Wright (2012)[838] the formulation of the provision certainly gives a wrong and limiting message to the industry since it does not include any reference to the different aspects of privacy but only to data protection.

As designed, DPIA should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of the data subject by virtue of their nature, scope or purposes.[839] In this way it covers relevant systems and processes of processing operations, but not individual cases.[840] As a result it seems that it will operate more as a risk-solutions assessment for systems of surveillance and processors and it would not influence the choice for the surveillance

[834] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995, pp. 0031-0050

[835] See Article 20 of the Data Protection Directive; Le Grand, G., Barrau, E. (2012), Prior checking, a forerunner to privacy impact assessments, in Wright and De Hert eds., *Privacy Impact Assessment*, Springer, pp. 97-116

[836] A model of DPIA on the basis of the GDPR is presented in: Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M. (2016) A Process for Data Protection Impact Assessment under the European General Data Protection Regulation, in Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (Eds.) *Privacy technologies and policy*, pp. 21-37

[837] De Hert, P. (2012), A human rights perspective on privacy and data protection impact assessment, in Wright and De Hert eds., *Privacy Impact Assessment*, Springer, pp. 33-76

[838] Wright, D. (2012), The state of art in privacy impact assessment, *Computer Law and Security Review*, vol. 28, pp. 54-61

[839] Article 27 Directive 2016/680

[840] Recital 58 Directive 2016/680

technology used in the specific cases. It will thus have only a marginal effect for solving the problem of the proportionality of surveillance measures.

Both prior checking as well as the data protection impact assessment give limited information on surveillance possibilities related with technical features of the devices. They have a limited scope of application focusing only on data protection and covering only one of the aspects of privacy, namely privacy of personal data. For these reasons, it is argued that the information that results from these methods does not satisfy the needs of national oversight authorities in light of the proper use of the proportionality principle.

5.3.3.2 Privacy Impact Assessment

Another method used in a number of States and proposed to be introduced at European Union level is the Privacy Impact Assessment (PIA). It is considered as an important tool for assessing privacy implications of different devices. PIAs can be defined as: "*a methodology for assessing the impacts on privacy of a project, policy, programme, service, product, or other initiative and, in consultation with stakeholders, for taking remedial actions that are necessary to avoid or minimize negative impacts*".[841] PIAs are seen as an early warning system, to identify possible privacy implications of new devices preferably at a stage that still permits the intervention in the project in order to amend them. PIAs are regarded to help to ensure that privacy is designed as a characteristic of the new devices.[842]

According to Clarke (2009), the concept of PIAs started to emerge and mature in the period 1995-2005.[843] In the EU, as already seen above, the Data Protection Directive does not make direct reference to PIAs, but only to a prior checking.[844] The introduction of a PIA in the EU was suggested by the European Commission in 2009 in a recommendation on the radio frequency identifiers (RFID). This was followed in 2011 by an act of the Article 29 Working Party approving a PIA framework and further developed by an industry group for RFID.[845] As for the Member States, the United Kingdom is the most active one and in 2007 introduced the PIA Handbook commissioned by the UK Information Commissioner's Office. Finland and Ireland as well appear to be moving in the direction of PIAs.[846]

[841] Wright, D. (2012), The state of art in privacy impact assessment, *Computer Law and Security Review*, vol. 28, pp. 54-61

[842] Waters, N. (2012), Privacy impact assessment – Great potential not often realized, in Wright and De Hert eds., *Privacy Impact Assessment*, pp. 149-160

[843] Clarke, R. (2009), Privacy impact assessment: Its origins and development, *Computer Law and Security Review*, vol. 25, pp. 123-135

[844] See Article 20 of the Data Protection Directive; Le Grand, G., Barrau, E. (2012), Prior checking, a forerunner to privacy impact assessments, in Wright and De Hert eds., *Privacy Impact Assessment*, Springer, pp. 97-116

[845] Please note that in April 2013 the Article 29 Working Party released an opinion in which it was very critical and did not approve a PIA framework proposed for the smart electricity meters (Opinion 4/2013)

[846] Clarke, R. (2009), Privacy impact assessment: Its origins and development, *Computer Law and Security Review*, vol. 25, pp. 123-135

A benefit of the PIAs is that they focus on the devices themselves. According to some authors, however, existing models focus almost entirely on data protection, not covering the other aspects of privacy.[847] This is also reflected in the new Data Protection Reform Package which limits the assessment method to only a data protection impact assessment. Since PIAs are designed to be conducted at a very early stage of a project and because of their nature and aim, it is not clear how they would operate when new privacy implications of a device are identified at an advanced stage, especially when the devices are already in the hands of the users. From a comparative analysis of PIAs in Australia, New Zealand, Canada, USA, Ireland and the UK with the aim of making the best suggestions for designing a European one, it is suggested, however, that a PIA will be most beneficial if it is considered as an ongoing process that should continue until and even after deployment of the project.[848] Thus far PIAs are supposed to be undertaken by the project developers with the result that the authority or company selected will have its influence and interest in the outcome. Also the making public or not of the results of a PIA is still under discussion.[849] One can argue that their publication will influence the awareness of the individuals on the fundamental rights implications of the devices they have in their hands. The currently discussed design of PIAs is thus of limited help for oversight authorities that need the results of the assessment for the proper use of the proportionality principle.

5.3.3.3 Surveillance Impact Assessment

A surveillance impact assessment (SIA) was first suggested in a report for the British Information Commissioner by the Surveillance Studies Network. The idea for this new method came from the identified necessity: "*to encompass the potential harmful effects of surveillance on a wider basis than that of protecting privacy*".[850] SIA was suggested to assess the impacts of surveillance on a range of values that may include, but also transcend, from privacy itself. For this it was suggested to develop PIA tools beyond their existing configuration. The 29 questions drafted by Marx (1998) for determining the ethics of surveillance were suggested as a starting point for designing a SIA.

The SIA method was further developed in 2012 by Wright and Raab.[851] Contrary to what its denomination would suggest, a SIA does not focus on the impact on surveillance of a new project or device, but makes a social, economic, financial, political, legal, ethical and psychological impact of

[847] Wright, D. et al. (2010), Sorting out smart surveillance, *Computer law & Security review*, vol. 26, pp. 343-354
[848] Wright, D., Finn, R., Rodrigues, R. (2013) A comparative analysis of Privacy Impact Assessment in six countries, *Journal of Contemporary European Research*, vol. 9, no. 1, pp. 160-180
[849] Wright, D., De Hert, P. (2012), Introduction to Privacy Impact Assessment, in Wright and De Hert (eds.), *Privacy Impact Assessment*, pp. 3-32
[850] See: Raab, C., Ball, K., Graham, S., Lyon, D., Murakami Wood, D., Norris, C. (2006) 'Report on the Surveillance Society' for the information Commissioner's Office, available online at: http://www.surveillance-studies.net/?page_id=3 (last accessed: 2.5.2013)
[851] Wright, D., Raab, C.D. (2012), Constructing a surveillance impact assessment, *Computer Law and Security review*, vol. 28, pp. 613-626; Raab, C.D, Wright, D. (2012), Surveillance: Extending the limits of Privacy impact assessment, in Wright and De Hert (eds.), *Privacy Impact Assessment*, pp. 363-383

surveillance for individuals or society as a whole. SIA has therefore the focus not on the devices, but on the subjects of surveillance, being these individuals or entire groups of population.

The methodology of SIA was further developed in the SAPIENT project where its purpose is presented as: "*to assess the risks that a surveillance related project, policy, programme, service, product or other initiative poses for privacy, as well as for other human rights and ethical values*".[852] The method is proposed to be used when a new surveillance project is contemplated or an existing surveillance system is to be modified or expanded. Its focus is therefore on surveillance technologies, systems and applications and not on other devices that are not built for the purpose of surveillance.

As it was briefly described above, the method is principally directed towards identifying the impact of surveillance projects on individuals or society as a whole, not the surveillance capabilities of devices.[853] In addition, it appears that the definition "surveillance projects" is limited to projects designed for the purpose of surveillance and is not extended to devices we use daily, that are not designed for the purpose of surveillance but can be used for such purposes. This conclusion derives also from the fact that the ones that are required to undertake a SIA are identified as: developers of surveillance systems, the ones who commission the design of surveillance systems and regulators that want to assess surveillance systems proposals. This method is therefore having only a limited value for guiding the proper use of the proportionality principle by national authorities in cases of surveillance with non-purpose built technology.

5.3.3.4 A model for assessing the privacy ´cost´ of a surveillance system

A model for assessing the privacy ´cost´ of a surveillance system was elaborated by Thommesen and Andersen (2009).[854] The model comes closer to the idea expressed in this study for a method that will aid the identification of the needed information for national authorities that issue surveillance authorizations. The model offers a matrix for establishing the intrusiveness of different surveillance systems. The authors start by listing the dimensions of privacy: (i) privacy of personal behaviour; (ii) privacy of location and space; (iii) privacy of the person; (iv) privacy of personal data, and (v) privacy of personal communication. It is to be noticed that "privacy of location and space" was not included in the work on the types of privacy from Clarke (2006).[855] Due to technology advances, however, also other authors consider the division of Clarke as outgrown and propose to add three more types of privacy to his original list: "privacy of location and space", "privacy of thoughts and feelings" and

[852] Wright et al. (2014) SAPIENT Deliverable 4.4: A guide to surveillance impact assessment – How to identify and prioritise risks arising from surveillance systems, available online at: http://www.sapientproject.eu/D4.4%20-%20SIA%20Manual%20(submitted%2001%20August%202014).pdf (last accessed: 11.6.2015)

[853] Wright, D., Raab, C.D. (2012), Constructing a surveillance impact assessment, *Computer Law and Security review*, vol. 28, pp. 613-626

[854] Thommesen, J., Andersen, H.B. (2009), Privacy implications of surveillance systems, available online at: http://orbit.dtu.dk/fedora/objects/orbit:56150/datastreams/file_4010841/content (last accessed: 6.5.2013)

[855] Clarke, R. (2006), What's 'Privacy'?, available online at: http://www.rogerclarke.com/DV/Privacy.html (last accessed: 10.07.2013)

"privacy of association (including group privacy)".[856] Only the first type is however considered in the matrix designed by Thommesen and Andersen. This is the reason it is considered as not covering all known aspects of the protected private life of the individuals.

The authors then identify the ways privacy can be invaded and distinguish three types of invasion: physical intrusion, observation and, acquisition of personal information from others. The degree of intrusiveness of different surveillance methods is then established as the outcome of seven different dimensions of surveillance. First the nature of the observer, then the degree of personal identification, the place surveillance is performed, the sensitivity of the collected information, its degree of accuracy, the purpose of surveillance and last, the awareness of the observed subject are assessed. The authors stress the possibility that the method might be useful also for the analyses of ethical aspects of surveillance systems and might aid in foreseeing problems and reactions that may not be identified before the system is implemented.

The matrix created has the benefit of covering more aspects of privacy than the other methods discussed so far. But it does not cover them all. This is however not the only complain to the designed matrix. When dealing with the dimensions of surveillance, it covers only 7 of them while other authors, as for example Marx (2002),[857] have been identifying 26 dimensions. The matrix does not offer the possibility for comparing alternative surveillance devices nor does it allow for identifying the effects that a surveillance system might have on the invasion of privacy of third parties. The matrix is also not offering the possibility to assess possible linkages of collected data with other systems that will make the information resulting from the combination more intrusive and dangerous in terms of the violation of the right to privacy. The guidance that this model of privacy assessment gives to national authorities is limited and does not solve the existing problem that they face when assessing the proportionality of their decisions.

5.3.4 A fundamental rights approach of privacy assessment methods

In the previous sub-section were discussed a number of privacy assessment methods that are adopted (e.g. prior checking, DPIA), or are proposed to be adopted in the European Union (e.g. PIA). In this sub-section, it is argued from a fundamental rights perspective why none of these methods satisfy the identified need of the oversight authorities for information on the surveillance abilities of the devices.

The private life of the individuals is protected as a fundamental right in the European Union. Even if the legal provisions allow a limitation of this right by State authorities, it is important that any

[856] Wright, D., Raab, C.D. (2014), Privacy principles, risks and harms, *International Review of Law, Computers and Technology*, vol. 28, no. 3, pp. 277-298

[857] Marx, G. (2002), What is new about "New surveillance"? Classifying for change and continuity, *Surveillance and Society*, vol. 1, no. 1, pp. 9-29

limitation of the right is done lawfully. The proportionality principle is the one indicated by the laws, courts' decisions and doctrine to guide national authorities when adopting a decision for limiting a fundamental right.

Since the proportionality principle does not have a normative value, it is important that national authorities have *ex ante* at their disposition all the needed information for adopting proportionate decisions. In sub-section 5.3.1 it is argued that it is difficult to apply the legal safeguards for the proportionality principle properly *ex post* because of the implications that derive from the flexibility of the principle and the margin of discretion that national authorities enjoy.

From a fundamental rights' perspective, it is clear that lawful interferences with the private sphere of the individuals are to be done in the way that restricts and interferes the least with the individuals´ rights. Considerations of efficiency are to be less of a concern in such decisions. For complying with such a requirement, national oversight authorities must be aware first of all of the alternative devices that can be used for reaching the same goal and select among them the one that interferes the least with the rights of the individuals. For this it is important to identify the aspects of the private life with which devices used for surveillance will interfere. In addition, for establishing their level of intrusiveness, an evaluation of the dimensions of surveillance with which these devices have an impact needs to take place. The effects of the surveillance measure for third parties need to be identified as well.

Regarding the aspects of privacy, it was seen that thus far the existing and proposed assessment methods do not cover all these aspects. Prior checking, DPIA and PIA focus mainly on data protection aspects of the devices and not on privacy as such. As it was mentioned earlier, it almost looks like the European legislator wants to equalize the right to data protection with the one to privacy. This is quite surprising not only because privacy and data protection are presented as two separate rights in the European Charter of Fundamental Rights (articles 7-8) but also because of their different scope. The right to privacy aims to protect the private life of individuals from arbitrary interferences of State actors, while the right to data protection focuses on the fair and legitimate collection and processing of personal data.[858] It is true that in certain situations the two rights might overlap with each other, but even in such situations the right to privacy would focus on the aspects of the private life that have been interfered with and the way this is done while the right to data protection would focus on the way the personal data are treated. The SIA method on the other side does not focus on devices as such, but on the subjects of surveillance and on the effects the surveillance activity has on them. Also the fact that its methodology points on the fact that the method is designed to focus on surveillance related projects or products, excludes from its scope of application devices not built for the purpose of surveillance. The model for assessing the privacy 'costs' of a surveillance system has also its deficits with this regards. It focuses only on limited aspects of privacy and not on all the ones identified thus far.

[858] Mitsilegas, V. (2015) The transformation of privacy in the area of pre-emptive surveillance, *Tilburg Law Review*, vol. 20, pp. 35-57

Regarding the dimensions of surveillance, it was seen that prior checking, DPIA and PIA are not directed to law enforcement authorities. As a result, they also do not focus on the dimensions of surveillance. SIA focuses on the ethics of surveillance and aims to present a social, economic, financial, political, legal, ethical and psychological impact of surveillance for individuals or society as a whole. However, since it does not focus on devices, it is not clear if it is able to establish in this way also the intrusiveness level of the different devices into the life of the individuals. The model for assessing the privacy 'costs' of a surveillance system on the other side covers only a limited number of the dimensions of surveillance (only 7) while other authors identify 26 of them.

The interference that devices not built for surveillance have with the private life of individuals that are not the target of the surveillance authorisation, is not considered in any of the explored methods. From the above elaboration it can be said that the existing methods of privacy assessment of devices, from a fundamental rights point of view, do not satisfy the need of national oversight authorities for information that would enable them to adopt proportionate decisions.

5.3.5 Concluding remarks

National structures of surveillance oversight play an important role with regards to the authorization of surveillance mandates. These authorities must have the possibility to make a proper *ex ante* evaluation of the measures they authorize which has to follow the legal rules and the proportionality principle. A proper *ex ante* evaluation of the surveillance measures and devices to be used is evaluated as more important than an *ex post* evaluation because, apart the shortcomings of the latter, it would also, and first of all, save the individuals the risk of having their fundamental rights infringed.

While there is not a distinction between structures of surveillance oversight that would operate for cases of traditional surveillance and for cases of surveillance with non-purpose built technology, the proper use of the proportionality principle is more sensitive in cases of authorizations for surveillance with non-purpose built technology. This is because the choice of non-purpose built technology for surveillance might have more severe implications with regards to the aspects of the private life of the individual that are being interfered with, the level of interference, as well as interference with the life of third parties.

A number of methods are in operation or designed in the EU for assessing the impact of technology with the private life. These methods are however mainly limited to a data protection point of view and do not take into account the need that national oversight authorities have for information. For these reasons a new method, to guide national authorities on the surveillance properties and privacy implications of the devices that they authorize for use in specific situations, is needed.

This new method must, first of all, be able to identify all alternative devices that might be used for reaching the same result. The alternative devices must be assessed in light of the different privacy aspects, for establishing the aspects of the private life of the individuals with which they interfere. They must also be assessed in light of the dimensions of surveillance in order to compare their level of intrusiveness into the individuals´ private life. The method has to take into account possible data combination as well as interferences with the private life of third parties. The DPIA prescribed in the new Data Protection Directive might serve as one of the steps of this impact assessment. To complete the theoretical framework of this assessment method, however, further research is needed.

It is difficult to expect in one person a full understanding of how laws, policies and technologies operate simultaneously. It would thus be better to have the design of such a method done from more than one person and with the possibility to cover all different fields. However, only when national oversight authorities will have the needed information on the technologies they authorize to be used for limiting the rights of the individuals, can we expect that the fundamental right to privacy will be safeguarded in conformity with the proportionality principle.

5.4 Discussion and conclusion

Surveillance with non-purpose built technology has characteristics that distinguish it from traditional surveillance. This is not reflected however thus far in the law and the case law at European level. The aim of this chapter was to explore the law enforcement access to information available via non-purpose built technology as well as the structures of surveillance oversight and to assess if they adequately deal with this form of surveillance.

Surveillance with non-purpose built technology increases the possibilities for law enforcement authorities to obtain the data from private parties, as for example service providers, which have access to them. This possibility does not change, however, the legal obligations of the authorities to operate in conformity with the legal rules and to respect the existing safeguards for the individuals. At the same time, makes private parties that process data for the purpose of law enforcement fall under the legal regime that regulates the latter.

Also the reasonable expectation to privacy that individuals have must not change in cases of the use of non-purpose built technology for surveillance purposes. Even though often the technology blurs the distinction between what is considered as private and what is available to other parties, the case law of the European Court of Human Rights has clarified that it is the systematic or permanent collection of the information as well as the use of technology beyond its foreseeability that brings even activities that take place in public to fall into the realm of privacy protection.

Apart the access to information other sensitive issues for surveillance with non-purpose built technology are the structures of surveillance oversight. These structures operating at national level are the ones that authorize the use of surveillance measures and devices and must take their decisions in compliance with the applicable laws and with the proportionality principle.

Currently these structures do not have the information that they need for taking proportionate decisions and the current methods of privacy assessment of technology are unable to provide it. There is the need of a new privacy and data assessment method to aid oversight structures for taking proportionate decisions that imply the use of technology.

In conclusion, it can be said that for safeguarding the right to privacy in cases of surveillance with non-purpose built technology when authorizing for and accessing the data the existing legal framework and the general principles of law are not enough. In this chapter were identified additional principles that must be taken into account. For the safeguarding of the right to privacy, private parties that have access to the collected data and collaborate with law enforcement must fall under the same rules and requirements as State authorities. An independent layer of review by a judicial or independent administrative body is required to limit the discretion of law enforcement. Any surveillance authorization must follow a privacy impact assessment of the technology that is proposed for use in the specific surveillance case.

Chapter 6 Conclusion

6.1 Introduction

During the period of time in which this research was completed Europe and its citizens faced a number of events that made the general feeling on security and on the fundamental rights to privacy and data protection fluctuate at different occasions. These events were on one side linked with the operating of intelligence bodies and the security of individuals in cases of terrorist attacks (as it was the case in 2015 in Paris with a series of attacks that killed more than 100 individuals and wounded many more,[859] or in 2016 in the airport and the metro of Brussels that killed 35 and wounded 300),[860] and on the other side with major revelations on the existence of global surveillance programmes (as it appeared from the release of a number of secret documents from Edward Snowden in 2013).[861] These events influenced the original thinking process for this work and, in a certain way, made the completion of the study even more pressing than it was at the time it started.

Also the legal framework changed in the meantime. This was the result of a number of judgements from the Court of Justice of the EU as for example: the invalidation of the Data Retention Directive,[862] the introduction of the so called `right to be forgotten`,[863] the *Schrems* decision which invalidated the Safe Harbour arrangement governing data transfers between the EU and the US,[864] etc. as well as of legislative developments. The draft Data Protection package and all the lobbying process around it which was presented vividly in the media and the doctrinal debate coexisted almost parallel with the research till its adoption in May 2016.[865] In addition, new legislative developments are seen in the horizon. A draft proposal for extending the EU Regulation on exporting dual use items to regulate also items that have a potential to be used for infringements of fundamental rights, thus also for

[859] Phipps, C., Rawlinson, K. (2015) Paris attacks kill more than 120 people – as it happened, in *the Guardian,* 14 November 2015, available online at: https://www.theguardian.com/world/live/2015/nov/13/shootings-reported-in-eastern-paris-live (last accessed: 2.8.2016)

[860] Shanon, V. (2016) Brussels attacks: What we know and what we don't know, in *New York Times*, 22 March 2016, available online at: http://www.nytimes.com/2016/03/23/world/europe/brussels-attacks-what-we-know-and-dont-know.html?_r=0 (last accessed: 2.8.2016)

[861] Greenwald, G., MacAskill, E. (2013) Boundless Informant: the NSA's secret tool to track global surveillance data, in the Guardian, 8 June 2013, available online at: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (last accessed 2.8.2016); Greenwald, G., MacAskill, E. (2013) NSA Prism program taps in to user data of Apple, Google and others, in *the Guardian*, 6 June 2013, available online at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (last accessed: 2.8.2016)

[862] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238

[863] C-131/12 Google Spain EU:C:2014:317

[864] C-362/14 Schrems v. Data protection Commissioner EU:C:2015:650

[865] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, pp. 1–88; Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp. 89–131

surveillance purposes, was presented by the EU Commission in September 2016.[866] A draft for the new e-Privacy Regulation was published in the beginning of 2017.[867] On the back of all these, technology did of course continue its development with high speed and new ways for interfering with the private life of the individuals are developing.[868]

All these developments reinforced the importance of this study and the completion of the research agenda posed at the beginning of this work. After this short introduction, in the following section (6.2) the answers to the main research question and the sub-questions are given in turn. In section 6.3 are presented the recommended safeguards for service providers and other parties that have access to data collected with non-purpose built technology as well as for state authorities that issue surveillance mandates and for law enforcement authorities. These recommendations derive from the studied EU legal framework and the European jurisprudence as well as the identified challenges to the right to privacy. The final conclusions are presented in section 6.4.

6.2 The answers to the research questions

This research had the aim to asses if the current European legal framework provides adequate protection of the fundamental right to privacy of the individuals against the threats created by law enforcement's surveillance with non-purpose built technology. To fulfil this objective the European legal framework was assessed theoretically and with the help of three case studies: smart meters, smart phones and stand-alone GPS navigation devices.

At the end of the research it can be said that the European legal framework is not adequate for protecting the right to privacy of the individuals in those situations in which non-purpose built technology is used by law enforcement for the scope of surveillance. In this study were identified a number of factors that determine the reaching of this conclusion. Firstly, surveillance with non-purpose built technology has characteristics that distinguish it from traditional surveillance. These characteristics make the interference with the rights of the individuals more intensive and severe than cases of traditional surveillance. The technology neutral nature of the laws at European level leads to surveillance with non-purpose built devices being treated in the same way as traditional surveillance. As a result, in those cases in which law enforcement authorities use non-purpose built devices for surveillance, the rights of the individuals are less protected. Secondly, even though it is agreed and declared that any interference with the fundamental rights of the individuals must

[866] Stupp, C. (2016) Commission plans export controls for surveillance technology, available online at: https://www.euractiv.com/section/trade-society/news/technology-companies-face-export-hurdles-under-draft-eu-rules/ (last accessed: 2.8.2016)
[867] Stupp, C. (2016) Commission to propose reform of ePrivacy directive in 2017, available online at: https://www.euractiv.com/section/digital/news/commission-to-propose-reform-of-eprivacy-directive-in-2017/ (last accessed: 2.8.2016)
[868] See for example Hern, A. (2016) Your battery status is being used to track you online, in *the Guardian,* 2 August 2016, available online at: https://www.theguardian.com/technology/2016/aug/02/battery-status-indicators-tracking-online (last accessed: 2.8.2016)

comply with the principles of necessity and proportionality, in this study it was argued that by not focusing on the technology used, it is impossible for national authorities to assess the proportionality of a surveillance mandate. Thirdly, the secondary EU legislation focuses on data protection leaving the regulation of the right to privacy to the primary provision of article 7 of the Charter (and article 8 of the Convention) as well as to the standards set in the case law of the European Court of Human Rights. In this study, it was argued that this is not enough for ensuring an equal level of protection of the right throughout the European Union.

For reaching the above conclusion, a number of sub-research questions focusing on particular aspects of the main research question were addressed. The sub-research questions analysed: a) if there are legal characteristics differentiating traditional forms of surveillance from surveillance with non-purpose built technology; b) if the European legal framework that applies to traditional surveillance covers also the challenges that surveillance with non-purpose built technology creates; c) if the current structures of access to information allow disclosure for the use and the scope of surveillance with non-purpose built technology; d) if the current structures of surveillance oversight at European level adequately address surveillance with non-purpose built technology. The results of the research on each of these sub-questions are presented below.

a) Differences between traditional surveillance and surveillance with non-purpose built technology

Non-purpose built technology used for surveillance does not only have an effect on the quantity and the quality of the data collected. It also has an effect on the way surveillance is conducted (as it was seen in the case studies) and it creates new challenges for safeguarding the right to privacy of the individuals. Surveillance with non-purpose built technology is thus different from traditional surveillance on different aspects. It is submitted that due to the aspects that are listed below, surveillance with non-purpose built technology must be recognised as a specific form of surveillance.

Firstly, surveillance with non-purpose built technology turns law enforcement surveillance from a vertical to a horizontal activity. It involves as active subjects of surveillance a number of private parties that are not involved in traditional surveillance situations, as for example service providers, or it introduces even situations of self-surveillance. Secondly, the passive subject of surveillance changes from a well identified one to an unknown one. This is due to the increased situations of untargeted mass surveillance as well as of situations of incidental surveillance. Thirdly, surveillance is performed more often in the form of dataveillance. Fourthly, the aspects of the private life of the individual with which it is interfered, as well as the level of their interference is increased. Lastly, it makes surveillance an activity that is not limited in observing the present but that can easily go back in time for retrieving and analysing the past behaviour of individuals at a time in which a surveillance mandate was not issued or justified and may even serve for predicting future behaviour.

In addition, surveillance with non-purpose built technology creates more possibilities for incidental surveillance, for extended use of mass surveillance and for retroactive surveillance. These situations create new challenges for the protection of the right to privacy of the individuals and, from a first assessment, it was seen that they are not properly addressed in the current European legal framework.

b) The European legal framework applying to surveillance with non-purpose built technology

The European legal framework applicable to the field is fragmented between different international organisations (EU/CoE) as well as within the EU due to the former pillar structure. Surveillance, being this traditional or with non-purpose built technology, is seen as a national activity and left for regulation to the Member States. However, law enforcement operation is not a completely national affair. There are various sector-specific legislative instruments in the field that regulate police and judicial co-operation in criminal matters, in particular those governing the functioning of bodies created for facilitating collaboration between the Member States (e.g. Europol) which either contain particular data protection regimes, and/or which usually refer to the data protection instruments of the Council of Europe.

The rights to privacy and data protection, on the other side are protected at European level. It can be said, though, that while the right to data protection is regulated in various secondary pieces of legislation, the right to privacy is left with the general regulation of the primary laws and the judicial decisions. Data protection rules focus mainly on the treatment of data once they are in the hand of law enforcement. As discussed in section 3.4, these rules protect the right to privacy only in those cases in which non-compliance with data protection standards amounts to an infringement of the right to information privacy of the citizens. Focusing mainly on data protection has thus left many aspects of the right to privacy *de facto* unregulated and unprotected.

The new Data Protection Directive that will become effective as of May 2018, covers the activities of law enforcement for prevention, detection, investigation and prosecution of crime. Being designed in a technology neutral fashion it covers surveillance performed with traditional as well as with non-purpose built technology. The scope of the application of the Directive is limited, however, to the field of data protection leaving the protection of the right to privacy outside its reach. The protection of the right to privacy remains highly guided from the article 8 ECHR and the elaboration of the right by the Court of Justice of the EU decisions and the test to identify arbitrary State interferences established by the European Court of Human Rights. Since, as analysed in section 3.4, the right to privacy is different from the right to data protection, any attempt of the legislator to regulate privacy by addressing only the protection of the right to data protection is just an illusion.

It can be finally said that in as far as the European legislation covers State surveillance activities, in general, it covers also surveillance with non-purpose built technology. The scope of the legislation is

however limited and it does cover the protection of the right to privacy as such, nor does it have special safeguards for the situations of incidental surveillance, mass surveillance and retroactive surveillance which are associated with surveillance with non-purpose built technology.

c) Law enforcement access to information collected with non-purpose built technology

Information collected with non-purpose built technology is accessible by law enforcement. This regards cases in which the data are collected by law enforcement itself as well as those cases in which the data are collected by private parties and transferred to law enforcement authorities. Any time that there is an interference with the rights of privacy and data protection of the individuals the general safeguards established at European level in the legal rules and in the jurisprudence, apply. This standard of protection must not change when the information is transferred by private parties to law enforcement, nor in those situations in which the individuals expose their data to the public by not setting proper privacy protection filters. Though not established explicitly in the legal rules, the case law from the European Court of Human Rights shows that the right to privacy has to be protected in all situations.

From the analyses of the case law it can be concluded that the use of non-purpose built technology for surveillance must be treated in a similar fashion with situations in which a person is not reasonably expected to foresee the use of technology beyond its normal use. Such situations belong to the realm of privacy protection and must benefit from, at least, the same safeguards designed for the protection of privacy and personal data in general. Thus, the proliferation of technology that has a potential to be used for surveillance purposes and its use by law enforcement authorities should not lower the standards created for safeguarding the right to privacy of the individuals.

d) The capability of structures of surveillance oversight to deal with cases of surveillance with non-purpose built technology

Law enforcement needs authorisation for using for surveillance purposes non-purpose built technology in the same fashion as in cases of traditional surveillance. While there is not a distinction between the rules and structures of surveillance oversight that would operate for cases of traditional surveillance and for cases of surveillance with non-purpose built technology, the proper use of the proportionality principle is more sensitive in cases of authorizations for surveillance with non-purpose built technology. This is the result of the fact that the choice of non-purpose built technology for surveillance might have more severe implications with regards to the aspects of the private life of the individual that are being interfered with, the level of interference, as well as interference with the life of third parties.

A proportionate decision authorising the technology to be used for surveillance requires an assessment of the implications that this has for the right to privacy of the individuals as well as the

choice for the less intrusive instrument. A number of methods are in operation or designed in the EU for assessing the impact of technology to the private life. These methods are, however, mainly limited to a data protection point of view and do not take into account the need that national oversight authorities have for information. For these reasons a new method, to guide national authorities on the surveillance properties and privacy implications of the devices that they authorize for use in specific situations, is needed.

This method must first of all be able to identify all alternative devices that might be used for reaching the same result. The alternative devices must be assessed in light of the different privacy aspects they interfere with. They must also be assessed in light of the dimensions of surveillance in order to compare their level of intrusiveness into the individuals´ private life. The method has to take into account possible data combination as well as interferences with the private life of third parties. To complete the theoretical framework of this assessment method, however, further research is needed.

6.3 Recommendations

Since the legal framework applicable at European level is found to be inadequate, the role of other actors for the protection of the fundamental right to privacy becomes prominent. As it was discussed in chapter 2 and confirmed by the case studies in chapter 4, non-purpose built technology used for surveillance gives private parties a prominent role in surveillance activities alongside law enforcement authorities. This is due to the fact that the data collected with non-purpose built technology are available with service providers or other third parties having access to them. In this section are presented a number of recommendations for safeguarding the right to privacy of the individuals. These recommendations are made in light of a human rights' based approach on the basis of the study of non-purpose built devices used for surveillance, of the rules and the legislation applicable at European level as well as of the case law of the Court of Justice of the EU and the European Court of Human Rights. With the aim to safeguard the right to privacy, these recommendations address the operation of service providers and other private parties that have access to the data, as well as the one of law enforcement and other State authorities that issue surveillance mandates.

a. Recommendations for service providers and other private parties that have access to the data

When talking about devices that are not built for the purpose of surveillance the first thought goes to the fact that these devices are in the hands of individuals and are managed by other private parties, as for example the service providers. Under the data protection rules these private parties qualify as data controllers. It was already seen that private parties that have access to the data and in this quality collaborate with State authorities fall under the same rules as the State authorities themselves. They must thus ensure that no interference with the private life of the individuals goes beyond what is necessary and proportionate. This is a first safeguard that intends to raise the accountability of private parties that have access to private data.

Service providers must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that any processing of the data is done in accordance with the new data protection regime.[869] In addition, national rules must regulate the period for which the data are retained, which must follow objective requirements,[870] and ensure the irreversible destruction of the data at the end of the data retention period.[871] For as long as there are no specific rules on retention of data, as it is for example the case with smart meters, the providers must keep only the data required for specific purposes (as for example taxation) and in the form required. For smart meter data and taxation purposes, for example, there is no need to keep the detailed data on the basis of which it is possible to retrieve activities taking place within a household but only the final consumption of energy.[872] Data retained by service providers for their company strategies must follow the principles of consent[873] and anonymization.[874] Substantive and procedural rules must be drafted on the access and the processing of the data.[875] It is also important to keep the data saved within the territory of the EU for avoiding that they could become subject to rules of other jurisdictions.[876] A data protection impact assessment must take place for identifying the risks to the right of the individuals when processing the data and enabling the service providers to properly comply with the data protection rules and regulations.[877]

b. Recommendations for authorities that issue surveillance mandates and law enforcement authorities

This research, and especially the case studies, showed that surveillance with non-purpose built technology creates challenges for the protection of the right to privacy of European citizens. Needless to add that any mandate for surveillance with these devices must be in conformity with the European rules and standards on the field. As regulated by article 8(2) ECHR and clarified further by

[869] Article 19(1) Directive 2016/680
[870] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 64
[871] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 67
[872] This is in accordance with data minimization principle that derives from article 6(1)(b) and (c) of Directive 95/46/EC
[873] Data Protection Directive 95/46/EC, article 2(h)
[874] There are studies, however, that show an easy possibility for re-identification of smart meter data in 68,3% of the cases. See Buchman, E., Boehm, K., Burghardt, T., Kessler, S. (2013) Re-identification of smart meter data, *Pers Ubiquit Comput*, vol. 17, pp. 653-662
[875] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 60
[876] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 68
[877] Commission Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems, OJ L 73, 13.3.2012, para. 4-9; see also European Commission, Smart Grid Task Force 2012-2014, Expert Group 2, Data protection impact assessment template for smart grid and smart metering systems, available online at:
https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf (last accessed: 4.1.2016) and its criticism by Article 29 Data Protection Working Party, Opinion 04/2013 on the Data protection impact assessment template for smart grid and smart metering systems prepared by Expert Group 2 of the Commission´s Smart Grid Task Force, 22 April 2013, available online at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (last accessed: 4.1.2016)

the case law of the European Court of Human Rights,[878] every interference with the right must be provided by the law and comply with the principles of necessity and proportionality. Keeping in mind the level of intrusion into the private sphere of the individuals that can be attained via the use of non-purpose built devices, it is recommended that in view of the surveillance potential of a device, the highest level of safeguards must be followed.

Any impact that the use of the data by law enforcement authorities has on the fundamental rights of the individuals must be assessed in detail and individuals must be informed *ex officio* on the data collected about them, when this does not have implications for the legal process. The European Courts thus far have not been exhaustively clarifying the definition of what has to be considered as 'necessary' but stay with the broad concept of a 'pressing social need'.[879] It is however clear that necessity is an important step of the proportionality test. A measure for being proportionate must be first of all appropriate or suitable to protect the interests that require protection. It must be necessary, meaning that no measure less restrictive must be available to attain the objective pursued. And it must be proportionate *stricto sensu*, meaning that the restriction that it causes must not be disproportionate to the intended objective or to the result that needs to be achieved.[880]

The criterion that the measure interfering with the private life must be the less restrictive alternative is important when deciding on issuing a surveillance mandate. The authorities issuing such mandates have to decide in light of the level of intrusion that the use of a device will have with the private life of the individual, with the possibility for the incidental involvement of other untargeted individuals (as for example guests of the household), as well as with the possibility of errors made during data processing. A privacy impact assessment method that would combine the privacy aspects with the surveillance dimensions would facilitate the burden of the authorities and guide for the adoption of proportionate surveillance mandates.

Finally, the surveillance mandates must be reviewed by a judicial or independent administrative body whose decisions would seek to limit access to the data to what is strictly necessary.[881] The involvement of such a body is in light with the proportionality principle and would limit the discretion of the law enforcement authorities.

[878] Kopp v. Switzerland, ECHR application no. 23224/94, 25 March 1998, para. 55; Perry v. The United Kingdom, ECHR application no. 63737/00, 17 July 2003, para. 55; Taylor, N. (2001) State surveillance and the right to privacy, in *Surveillance and Society*, vol. 1, no. 1, pp. 66-85

[879] Harris, D. et al. (2009), Law of the European Convention on Human Rights, Oxford University Press, second edition, p. 349

[880] Jans, J.H. et al. (2007), Europeanisation of Public Law, Europa Law Publishing, p. 149

[881] Joint cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others EU:C:2014:238, para. 62

6.4 Final conclusion

While technology advances by the minute, also the ways the private life of the individuals can be interfered with advance and proliferate. This study, and especially the three chosen case studies, showed the potential problems that arise from the use of non-purpose built technology for surveillance - especially the increased possibility for incidental surveillance, mass surveillance and retroactive surveillance. While the European legal framework is not adequate for dealing with these challenges, technology makes surveillance easy and cheap and law enforcement has increased possibilities for interfering with the private life of the individuals in ways that escape the current legal protection. Even though this study is not suggesting a prohibition for law enforcement authorities to use for surveillance purposes technology that is not built for that aim, the recognition of this special form of surveillance and of the challenges that it presents to the right to privacy by the laws, the courts, the policy makers and surveillance authorities would allow for an attentive assessment of the technology used for surveillance. Thus, the technology neutrality of the laws can be balanced by the technology awareness of all the other relevant actors.

A human rights' based approach suggests for the use of the surveillance measure and technology that interferes less with the private life of the individuals. As a result, the use of non-purpose built technology for surveillance must be scrutinized for ensuring that the necessary safeguards are followed. In addition, a regulatory framework for safeguarding the right to privacy can avoid unnecessary trade-offs and false dichotomies and demonstrate that both effective law enforcement and protection of fundamental rights can coexist.

Legal rules are often the result of a long legislative procedure and their final formulation reflects strongly the lobbying process that surrounded them. The safeguarding of the fundamental rights must thus not be the task of only one actor. Together with the legislators, also the courts, policy makers, law enforcement authorities, technology designers, individuals themselves, etc. must collaborate for the safeguarding of the rights. Even though the current legal framework in the European Union is not adequate for protecting the fundamental right to privacy of the individuals in cases of surveillance with non-purpose built technology, it contains a number of principles that serve for creating a bridge over the current gap created by the disconnection between the laws and the quickly advancing technology. These principles are:

a. Interference with the private life of the individuals must be limited to what it is proportionate and strictly necessary;
b. Law enforcement power to interfere with the private life of individuals must be supervised under a system of prior authorization;
c. Protection of privacy must be a design feature of all the technology;
d. An independent layer of review by a judicial or independent administrative body is required to limit the discretion of law enforcement;
e. Individuals must be informed about their collected personal data once this does not affect the legal process;

f. A continuous system of checks and balances is required for securing the protection of the fundamental rights of the individuals.

This study showed that in order to have the above listed principles work for safeguarding the right to privacy, they need to be complemented by a number of other principles that derive from the awareness that the nature of the technology effects the safeguarding of the fundamental right to privacy. These additional principles are:

a. The surveillance authorization must follow a privacy impact assessment of the technology that is proposed for use in a specific case;
b. Introduction of rules that change the purpose of data collection must be assessed both under data protection and privacy rules;
c. Technologies that do not comply with the privacy by design and by default criteria must not be used for surveillance;
d. In case of use for surveillance of devices that present different possibilities for interfering with the private life of the individuals, the highest level of safeguards must apply;
e. Private parties that have access to the data and that collaborate with law enforcement authorities must fall under the same rules and requirements as law enforcement authorities themselves.

Together, all these principles serve for safeguarding the right to privacy of the individuals at a time that technology advances with high speed and the laws are unable to foresee all future developments and protect the fundamental right to privacy of the individuals. Because, living in a democratic society, we can and must have at the same time effective law enforcement and protection of the fundamental right to privacy of the individuals.

Bibliography

Literature

Abel, W. (2009) Agents, Trojans and tags: The next generation of investigators, *International Review of Law, Computers and Technology*, vol. 23, no. 1-2, pp. 99-108

Alabdulkarim, L., Lukszo, Z. (2011) Impact of privacy concerns on consumers' acceptance of smart metering in the Netherlands, *IEEE*, pp. 287-292

Alonso Blas, D. (2010) Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom, *ERA Forum*, vol. 11, p. 233-250

Anderson, D., Murphy, C. (2011) The Charter of Fundamental Rights: History and prospects in post-Lisbon Europe, *EUI Working papers* 2011/08, August 2011

Anderson, R., Fuloria, S. (2010) On the security economics of electricity metering, in *Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS 2010)*, pp. 18

Arai-Takahashi, Y. (2002), The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR, Intersentia

Arthur, C. (2011) TomTom satnav data used to set police speed traps, in *The Guardian*, 28 April 2011, available online at: https://www.theguardian.com/technology/2011/apr/28/tomtom-satnav-data-police-speed-traps (last accessed: 15.4.2016)

Arthur, C., Garside, J. (2011) Smartphones take lead in European mobile phone market, *The Guardian*, 8 September 2011, available online at: http://www.theguardian.com/technology/2011/sep/08/smartphones-take-lead-in-mobile-phone-market (last accessed:20.1.2016)

Ashbrook, D., Starner, T. (2003) Using GPS to learn significant locations and predict movement across multiple users, in *Personal and Ubiquitous computing*, vol. 7, pp. 275-286

Bajaj, R., Ranaweera, S.L., Agrawal, D.P. (2002) GPS: Location tracking technology, *Computers*, vol. 35, no. 4, pp. 92-94

Balducci Romano, F. (2013) The Right to the Protection of Personal Data: A New Fundamental Right of the European Union, available online at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2330307 (last accessed: 15.4.2016)

Balough, C.D. (2011) Privacy implications of smart meters, Chicago-Kent Law Review, vol. 86, no. 1, pp. 161-191

Banerjee, S., Syed, Z., Bartlow, N., Cukic, B. (2015) Keystroke recognition, in. Li, S.Z, Jain, A.K. (eds.), *Encyclopedia of Biometrics*, pp. 1067-1073

Barak, A. (2012), Proportionality – Constitutional Rights and their limitations, Cambridge University Press

Bauman, Z., Lyon, D. (2013) Liquid surveillance: A conversation, *Polity Press*

BBC (2013) US NSA and UK GCHQ 'can spy on smartphones', 23 September 2013, available online at: http://www.bbc.com/news/world-europe-24009342 (last accessed: 8.2.2016)

Beckel, C., Sadamori, L., Staake, T., Santini, S. (2014) Revealing household characteristics from smart meter data, *Energy*, vol. 78, pp. 397-410

Bellia, P.L. (2008), The memory gap in surveillance law, *University of Chicago Law Review*, vol. 75, no. 1, pp. 137-179

Bennett D. (2012) The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations, *Information Security Journal: A Global Perspective*, vol. 21, no. 3, pp. 159-168

Bennett, C. (1996) The public surveillance of personal data: A cross-national analyses, in Lyon, D., Zureik, E. (eds.), *Computers, surveillance, and privacy*, pp. 237-259

Bentham, J. (1787) Panopticon or the Inspection House, in Bozovic, M. (eds.), *Panopticon Writings*, pp. 29-95, available online at: http://www.ics.uci.edu/~djp3/classes/2012_01_INF241/papers/PANOPTICON.pdf (last accessed: 16.03.2015)

Bergkamp, L. (2002) EU data protection policy - The privacy fallacy: Adverse effects of Europe´s data protection policy in an information-driven economy, *Computer Law & Security Report*, vol. 18, no. 1, pp. 31 - 47

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M. (2016) A Process for Data Protection Impact Assessment under the European General Data Protection Regulation, in Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (Eds.) *Privacy technologies and policy*, pp. 21-37

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F. et al. (2013) National programmes for mass surveillance of personal data in EU Member states and their compatibility with EU law, *Study submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf (last accessed: 1.11.2013)

Birnhack, M. (2013) Reverse engineering informational privacy law, *Yale Journal of Law and Technology*, vol. 15, no. 1, pp. 24-91

Blanke, J.-S., Mangiameli, S. (2013) The Treaty of the European Union - A commentary, Springer

Boehm, F., De Hert, P. (2012), Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law, *European Journal of Law and Technology*, vol. 3, no.3

Boekema, J. (2011), TNO Report - Assessment of the implementation regulations for Smart Meters, available online at: https://www.tno.nl/media/1050/assessment-of-the-implementation-regulations-for-smart-meters.pdf, (last accessed: 16.7.2015)

Bohli, J., Sorge, C., Ugus, O. (2010) On the security economics of the electricity metering, *Proceedings of 2010 IEEE International Conference on Communications Workshops*, pp. 10

Borton, D.A. et al. (2013) An implantable wireless neural interface for recording cortical circuit dynamics in moving primates, *Journal of Neural Engineering*, vol. 10, no. 2, pp. 16

Bowden, C. (2013) The US surveillance programmes and their impact on EU citizens' fundamental rights, *Briefing Note submitted to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs*, available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf (last accessed: 1.11.2013)

Brakel, R., van, De Hert, P. (2011) Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Cahiers Politiestudies*, vol. 3, no. 20, pp. 163-192

Brouwer, E. (2007), The use of biometrics in EU databases and identity documents, in Lodge, J. (eds.) *Are you who you say you are? The EU and Biometric Borders*, pp. 45-66

Brown, I., Korff, D. (2009) Terrorism and the proportionality of internet surveillance, *European Journal of Criminology*, vol. 6, no. 2, pp. 119-134

Buchman, E., Boehm, K., Burghardt, T., Kessler, S. (2013) Re-identification of smart meter data, *Personal and Ubiquitous Computing*, vol. 13, no.6, pp. 653-662

Bygrave, L. (1998) Data protection pursuant to the right to privacy in human rights treaties, *International Journal of Law and Information Technology*, vol. 6, pp. 247-284

Bygrave, L. (2008) International agreements to protect personal data, in Rule, J. B., Greenleaf, G. (eds.), *Global privacy protection*, Edward Elgar

Canalys (2006) Research Release 2006/81: Mobile GPS navigation market doubles year-on-year, available online at: http://www.gpsforensics.org/downloads/canalys_11aug06.pdf (last accessed: 21.4.2016)

Cannataci, J. (2009) Lex personalitatis and technology-driven law, *ScriptED*, vol. 5, no. 1, pp. 1-6

Cannataci, J. (2010) Study on Recommendation No. R(87)15 of 17 September 1989 regulating the use of personal data in the police sector – 'Data Protection Vision 2020: Options for improving European policy and legislation during 2010-2020', available online at: http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf (last accessed: 20.2.2015)

Cannataci, J., Caruana, M. (2013) Report: Recommendation R(87)15 Twenty-five years down the line, available online at: http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf (last accessed: 20.2.2015)

Casey, E., Bann, M., Doyle J. (2010) Introduction to windows mobile forensics, *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, vol. 6, no. 3-4, pp. 136-46

Cassa, C.A., Chunara, R., Mandl, K., Brownstein, J.S. (2013) Twitter as a sentinel in emergency situations: Lessons from the Boston Marathon explosions, *PloS Currents*, doi: 10.1371/currents.dis.ad70cd1c8bc585e9470046cde334ee4b

Cavoukian, A. (2013) Surveillance, then and now: Securing privacy in public spaces, available online at: https://www.ipc.on.ca/images/Resources/pbd-surveillance.pdf (last accessed: 26.4.2016)

Cavoukian, A., Polonetsky, J., Wolf, C. (2010), Smart privacy for the smart grid: embedding privacy into the design of electricity conservation, available online at: https://www.privacybydesign.ca/index.php/paper/smartprivacy-for-the-smart-grid-embedding-privacy-into-the-design-of-electricity-conservation/ (last accessed: 15.4.2015)

Chae, K., Kim, D., Jung, S., Choi, S., Jung, S. (2010) Evidence collecting system from car black boxes, in *Proceedings of the 7th IEEE conference on Consumer communications and networking conference*, pp. 254-255

Chalmers, D., Davies, G., Monti, G. (2014) European Union Law, Cambridge, 3rd edition

Chandler, J. (2009) Privacy versus National Security: Clarifying the Trade-off, in Kerr, I., Lucock C., Steeves, V. (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford University Press, pp. 121-138

Clarke, R. (1994) Dataveillance: Delivering '1984', in Green L., Guinery R. (eds.), *Framing Technology: Society, Choice and Change,* Allen & Unwin, available online at: www.anu.edu.au/people/Riger.Clarke/DV/PaperPopular.html (last accessed: 3.2.2015)

Clarke, R. (1997) Introduction to Dataveillance and Information Privacy, and Definitions of Terms, available online at: http://www.rogerclarke.com/DV/Intro.html (last accessed: 22.5.2014)

Clarke, R. (2006), What's 'Privacy'?, available online at: http://www.rogerclarke.com/DV/Privacy.html (last accessed: 17.6.2015)

Clarke, R. (2009), Privacy impact assessment: Its origins and development, *Computer Law and Security Review*, vol. 25, pp. 123-135

Clarke, R. (2015) Data retention as mass surveillance: The need for an evaluative framework, in *International Data Privacy Law*, available online at: http://idpl.oxfordjournals.org/content/early/2015/01/23/idpl.ipu036.full.pdf+html (last accessed: 17.6.2015)

Cohen, N. (2011) It's tracking your every move and you may not even know, *The New York Times*, 26 March 2011, available online at:

http://www.nytimes.com/2011/03/26/business/media/26privacy.html?_r=0 (last accessed: 22.5.2014)

Collins, T., Pearson, L., Delany, C. (2002) Rights-based approach, Discussion paper available online at: http://03559de.netsolhost.com/htmfiles/hill/17_htm_files/Committee-e/Tara-ARightsBased.pdf (last accessed: 10.2.2017)

Comey, J.B. (2014) Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?, available online at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (last accessed: 15.2.2016)

Cook, T. (2016) Open letter to customers, available online at: http://www.apple.com/customer-letter/ (last accessed: 11.3.2016)

Coster van Voorhout, J.E.B. (2006) Intelligence as legal evidence – Comparative criminal research into the viability of the proposed Dutch scheme of shielded intelligence witnesses in England and Wales, and legislative compliance with Article 6(3)(d) ECHR, *Utrecht law review*, vol. 2, no. 2, pp. 119 – 144

Coudert, F. (2014) Accountable Surveillance Practices: Is the EU Moving in the Right Direction?, in Preneel, B., Ikonomou, D. (eds.), *Privacy technologies and policy*, pp. 70-85

Coudert, F., Gemo, M., Beslay, L., Andritsos, F. (2011) Pervasive Monitoring: Appreciating Citizen's Surveillance as Digital Evidence, in *Legal Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention* (ICDP 2011), pp. 1–6

Covrig, C.F. et al. (2014) Smart Grids Projects Outlook, available online at: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf, (last accessed: 29.4.2015)

Cuijpers, C., Koops, B.J. (2012) Smart metering and privacy in Europe: Lessons from the Dutch case, in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds.), *European data protection: Coming of age*, pp. 269-293

Davis III, E.F., Alves, A.A., Sklansky, D.A. (2014) Social media and police leadership: Lessons from Boston, *New Perspective in policing,* available online at: http://www.hks.harvard.edu/content/download/67536/1242954/version/1/file/SocialMediaandPoliceLeadership-03-14.pdf (last accessed: 24.3.2016)

De Busser, E. (2009) Data protection in EU and US criminal cooperation, Maklu

De Busser, E. (2014) Privatization of information and the Data Protection Reform, in S. Gutwirth et al. (eds.), *Reloading data protection*, pp. 129-149

De Hert, P. (2005), Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, *Utrecht Law Review*, vol. 1, issue 1, pp. 68-96

De Hert, P. (2012), A human rights perspective on privacy and data protection impact assessment, in Wright and De Hert eds., *Privacy Impact Assessment*, pp. 33-76

De Hert, P., Boehm, F. (2012) The rights of notification after surveillance is over: Ready for recognition?, in Bus et al. (eds.), *Digital enlightment year book 2012*, p. 19

De Hert, P., Gutwirth, S. (2009) Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action, in Gutwirth, S., Poullet, Y., De Hert, P., Nouwt, J. & De Terwangne, C. (eds), *Reinventing Data Protection?*, pp. 3-44

De Hert, P., Gutwirth, S., Moscibroda, A., Wright, D., Gonzales Fuster, G. (2009) Legal safeguards for privacy and data protection in ambient intelligence, *Pers Ubiquit Comput*, vol. 13, pp. 435-444

De Hert, P., Koops, B.J., Leens, R. (2009) Constitutional rights and new technology: A comparative perspective, in Pawels, C. et al (eds), *Rethinking European media and communications policy*, pp. 319-350

De Hert, P., Papakostantinou, V. (2013) Three scenarios for international governance of data privacy: Towards an international data privacy organisation, preferably a UN agency?, *A Journal of Law and Policy for the Information Society*, vol. 9, no. 2, pp. 271-324

De Koster, P. (2005) Terrorism: special investigation techniques, CoE Publishing

De Schutter, O. et al. (2006) The Commentary of the Charter of Fundamental Rights of the European Union, available online at: http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf (last accessed: 2.5.2013)

De Souza e Silva, A., Gordon, E. (2014) Net locality, in Adey, P., Bissell, D., Hannam, K., Merriman, P., Sheller, M. (eds.), *The Routledge Handbook of Mobilities*, pp. 134-142

Decker, M. (2008) Location privacy – An overview, *IEEE Proceedings of the 7th Conference on Mobile Business*, pp. 221-230

Deflem, M. (2006) Europol and the policing of international terrorism: Counter-terrorism in a global perspective, *Justice Quarterly*, vol. 23, no. 3, pp. 336-359

Den Boer, M., Fernhout, R. (2008) Police oversight mechanisms in Europe: Towards a comparative overview of Ombudsmen and their competences, available online at: http://www.asef.org/images/docs/1270-Police_Oversight_Mechanisms_in_Europe.pdf (last accessed: 12.1.2016)

Dijk, A., van (2013) Retributivist arguments against presuming innocence, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 249-267

Distefano, A., Me, G. (2008) An overall assessment of mobile internal acquisition tool, *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, vol. 5 (supplement), pp. 121-127

Docksey, Ch. (2014) The European Court of Justice and the decade of surveillance, in Hijmans, H., Kranenborg, H. (eds.), *Data protection anno 2014: How to restore trust?*, pp. 97-111

Drulakova, R. (2006) Post-democracy within the EU: Internal security vs. human rights – unavoidable conflict?, paper prepared for the CEEISA 4th convention, Tartu, 25-27 June 2006, available online at:

http://www.ceeisaconf.ut.ee/orb.aw/class=file/action=preview/id=167766/Drulakova.doc, (last accessed: 1.11.2013)

Duckham, M., Kulik, L. (2007) Location privacy and location-aware computing, in Drummond, J. et al. (eds.), *Dynamic and Mobile GIS: Investigating Changes in Space and Time*, pp. 35-52

Duff, A. (2013) Who must presume whom to be innocent of what?, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 170-192

EDRi (2015) Non-exhaustive list of EU Member States with national legislation contrary to the Digital Rights Ireland Ltd (C-293/12) CJEU ruling, available online at: https://edri.org/files/DR_EDRi_letter_CJEU_Timmermans_20150702_annex.pdf (last accessed: 11.2.2016)

Eijkman, Q., Van Ginkel, B. (2011) Compatible or incompatible? Intelligence and human rights in terrorist trials, *Amsterdam Law Forum*, vol. 3, no. 4, pp. 1-16

Eissen, M. (1993), The proportionality principle in the case law of the European court of Human Rights, in Macdonald, R.St.J., Matscher, F. and Petzold, H. (eds.), *The European System for the Protection of Human Rights*, pp. 125-137

Enck, W. et al (2014) TaintDroid: An information-flow tracking system for real time privacy monitoring on smartphones, *ACM Transactions on Computer Systems*, vol. 32, no. 2, pp. 29

Enev, M., Gupta, S., Kohno, T., Patel, S. (2011) Televisions, video privacy, and powerline electromagnetic interference, *Proceedings of the 18th ACM Conference on computers and communications security*, pp. 537-550

Faraqui, A., Harris, D., Hledik, R. (2010) Unlocking the €53 billion savings from smart meters in the EU: How increasing the adoption of dynamic tariffs could make or break the EU's smart grid investment, *Energy Policy*, vol. 38, n. 10, pp. 6222-6231

Feiler, L. (2010) The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection, *European Journal of Law and Technology*, vol. 1, no. 3, pp. 1-34

Fenwick, H., Phillipson, G. (2011) Covert derogations and judicial deference: Redefining liberty and due process rights in counterterrorism law and beyond, *McGill Law Journal*, vol. 56, no. 4, pp. 863-918

Fink, U. (2014) Protection of privacy in the EU, individual rights and legal instruments, in Witzleb, N., Lindsay, D., Paterson, M., Rodrick, S. (eds.), *Emerging challenges in Privacy law*, pp. 75-91

Foucault, M. (1995) Discipline and Punish: The birth of the prison, Vintage Books

Friedewald, M. (2010) Sorting out smart surveillance, *Computer law and Security Review,* vol. 26, pp. 343-354

Fuchs, C. (2013) *Privacy and Security in Europe,* The Privacy & Security-Research Paper Series, Research Paper no. 6, available online at: http://www.projectpact.eu/privacy-security-research-

paper-series/privacy-security-research-paper-series/6_Privacy_and_Security_Research_Paper_Series.pdf (last accessed: 28.7.2016)

Galetta, A., De Hert, P. (2014) Complementing the surveillance law principles of the Court of Strasbourg with its environmental law principles. An integrated technology approach to a human rights framework for surveillance, *Utrecht Law Review*, vol. 10, no. 1, pp. 55 – 75

Gamino Garzia, A. et al. (2014) Study on Mass Surveillance – Risks and opportunities raised by the current generation of network services and applications, presented at European Parliament Scientific Foresight (STOA) Unit, December 2014, available online at: http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Study%20Mass%20Surveillance%20Part%201.pdf (last accessed: 23.2.2015)

Gellert R., Gutwirth S. (2013) The legal construction of privacy and data protection, in Computer Law & Security Review, vol. 29, no. 5, pp. 522 - 530

Gomez-Arostegui, H.T. (2005) Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations, *California Western International Law Journal*, vol. 35, no. 2, pp. 153-202

Gomez-Martin, L.E. (2012) Smartphone usage and the need for consumer privacy laws, Pittsburgh Journal of Technology Law, vol. 12, no. 2, pp. 1-21

Gonzalez Fuster, G. (2014) The emergence of data protection as a fundamental right of the EU, Springer

GPEN (2016) Privacy SWEEP on IoT, available online at: https://www.privacyenforcement.net/press-releases (last accessed: 9.11.2016)

Greenleaf, G. (2014) A world data privacy treaty? 'Globalisation' and 'modernization' of Council of Europe Convention 108, in Witzleb, N., Lindsay, D., Paterson, M., Rodrick, S. (eds.), *Emerging challenges in Privacy law*, Cambridge University Press, pp. 93-138

Greenwald, G., MacAskill, E. (2013) Boundless Informant: the NSA's secret tool to track global surveillance data, in the Guardian, 8 June 2013, available online at: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (last accessed: 2.8.2016)

Greenwald, G., MacAskill, E. (2013) NSA Prism program taps in to user data of Apple, Google and others, in *the Guardian*, 6 June 2013, available online at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (last accessed: 2.8.2016)

Greenwald, G., MacAskill, E., Poitras, L. (2013) Edward Snowden: the whistleblower behind the NSA surveillance revelations, *The Guardian* (9 June 2013), available online at: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance (last accessed: 20.1.2014)

Greer, S. (1997) The exceptions to Articles 8 to 11 of the European Convention of Human Rights, *Human Rights Files*, no. 15, Council of Europe Publishing

Greveler, U., Justus, B., Loehr, D., (2011) Multimedia Content Identification Through Smart Meter Power Usage Profiles, available online at: http://epic.org/privacy/smartgrid/smart_meter.pdf (last accessed: 27.4.2013)

Gutwirth, S. (2007) Biometrics between opacity and transparency, *Annals of the Italian National Institute of Health,* vol. 43, no. 1, pp. 61-65

Gutwirth, S., De Hert, P. (2006) Privacy, data protection and law enforcement. Opacity of the individual and transparency of power, in E. Claes, A. Duff & S. Gutwirth (eds.), *Privacy and the criminal law*, pp. 61-104

Gutwirth, S., Hildebrandt, M. (2010) Some Caveats on Profiling, in S. Gutwirth, Y. Poullet & P. De Hert. (eds.), *Data protection in a profiled world*, pp. 31-41

Harbo, T.I. (2010) The function of the proportionality principle in EU law, *European Law Journal*, vol. 16, no. 2, pp. 158-185

Hargreaves, T., Nye, M., Burgess, J. (2010) Making energy visible: A quantitative field study of how households interact with energy from smart energy monitors, *Energy Policy*, vol. 38, pp. 6111-6119

Harris, D. et al. (2009) Law of the European Convention on Human Rights, Oxford University Press, 2nd edition

Van Helburg, H., van (2014) RVO Report - Dutch Energy Savings Monitor for the Smart Meter, available online at: http://english.rvo.nl/sites/default/files/2014/06/Dutch%20Smart%20Meter%20Energy%20savings%20Monitor%20final%20version.pdf (last accessed: 16.7.2015)

Hern, A. (2016) Is the FBI v Apple PR war even about encryption?, in *The Guardian*, 23 February 2016, available online at: http://www.theguardian.com/technology/2016/feb/23/fbi-apple-pr-war-encryption-mobile-security (last accessed: 11.3.2016)

Hern, A. (2016) Your battery status is being used to track you online, in *the Guardian,* 2 August 2016, available online at: https://www.theguardian.com/technology/2016/aug/02/battery-status-indicators-tracking-online (last accessed: 2.8.2016)

Hijmans, H., Scirocco, A. (2009) Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be Expected to help?, *Common Market Law Review*, vol. 46, issue 5, pp. 1485–1525

Hildebrandt, M. (2014) Location Data, Purpose Binding and Contextual Integrity: What's the Message?, in Floridi, L. (eds.) *Protection of Information and the Right to Privacy - A New Equilibrium?*, pp. 31-62

Himma, K.E. (2007), Privacy vs. Security: Why privacy is not an absolute value or right, *San Diego Law Review*, vol. 45, pp. 859-922

Hirsch Ballin, M. (2008) An inside view of Dutch counterterrorism strategy: countering terrorism through criminal law and the presumption of innocence, *The Journal of the Institute of Justice and International studies*, vol. 8, pp. 139-151

Hoffmann, L. (1999), The influence of the European principle of proportionality upon UK law, in Ellis, E. (eds.), *The principle of proportionality in the laws of Europe,* pp. 107-115

Hofmann-Wellenhof, B., Lichtenegger, H., Collins, (1997) Global Positioning System: Theory and Practice, Springer, 4th edition

Husain M.I., Sridhar R. (2010) iForensics: Forensic analysis of instant messaging on smart phones, in Goel S. et al. (eds.) *Digital Forensics and Cyber Crime*, pp. 9-18

Hustnix, P. (2013) The Increasing Horizontal Impact of Personal Data Protection, *eucrim - The European Criminal Law Associations´ Forum,* no. 1, pp. 1-2

Hustnix, P. (2014) The reform of EU data protection: towards more effective and more consistent data protection across the EU, in Witzleb, N., Lindsay, D., Paterson, M., Rodrick, S. (eds.), *Emerging challenges in Privacy law*, pp. 62-71

Iqbal, M.U., Lim, S. (2008) Legal and ethical implications of GPS vulnerabilities, *Journal of International law and Technology*, vol. 3, no. 3, pp. 178-187

Iqbal, M.U., Lim, S. (2010) Privacy implications of automated GPS tracking and profiling, *IEEE Technology and Society Magazine*, pp. 39-46

Jacobs, F.G. (1999), Recent development in the proportionality principle in European Community law, in Ellis, E. (eds.), *The principle of proportionality in the laws of Europe,* pp. 1-21

Jans, J.H., et al. (2007), Europeanisation of Public Law, Europa Law Publishing

Jasserand, C.A. (2015) Avoiding terminological confusion between the notions of 'biometrics' and 'biometric data': an investigation into the meanings of the terms from a European data protection and a scientific perspective, *International Data Privacy Law*, pp. 1-14

Jenness, V., Smith, D.A., Stepan-Norris, J. (2007) Taking a look at surveillance studies, *Contemporary sociology: A Journal of Reviews,* vol. 36, no. 2, pp. vii-viii

Jeoen, W., Kim, J., Lee, Y., Won, D. (2011) A practical analyses of smartphone security, in Smith, M.J., Salvendy, G. (eds.), *Human interface*, pp. 311-320

Jones, K.B., Zoppo, D. (2014) A smarter, greener grid, Praeger

Jung, Y. (2014) What a smartphone is to me: Understanding user values in using smartphones, *Information Systems Journal,* vol. 24, no. 4, pp. 299-321

Kalogridis, G., Denic, S. (2011) Data Mining and privacy of personal behavior types in smart grid, *Proceedings of the 11th IEEE International Conference on Data Mining Workshops*, pp. 636-642

Kang, J., Shilton, K., Estrin, D., Burke, J., Hansen, M. (2012) Self-surveillance privacy, *Iowa Law Review,* vol. 97, pp. 809-847

Karim, W. (2004) The privacy implications of personal locators: Why you should think twice before voluntarily availing yourself to GPS monitoring, *Journal of Law and Policy, vol. 14, pp. 485-515*

Kearns, T. (1999) Technology and the right to privacy: The convergence of surveillance and information privacy concerns, *William & Mary Bill of Rights Journal*, vol. 7, no. 3, pp. 975-1011

Kilkelly, U. (2001), The right to respect for private and family life, Handbook no. 1, available online at: http://echr.coe.int/NR/rdonlyres/77A6BD48-CD95-4CFF-BAB4-ECB974C5BD15/0/DG2ENHRHAND012003.pdf (last accessed: 31.1.2013)

Kim, Y., Schmid, T., Srivastava, M., Wang, Y. (2009) Challenges in resource monitoring for residential spaces, *Proceedings of the first ACM Workshop on Embeded Sensing Systems for Energy-Efficiency in Buildings*, pp. 1-6

King, E. (2012) Civil servant admits British police grabbing location data of thousands of innocent people, available online at: https://www.privacyinternational.org/blog/civil-servant-admits-british-police-grabbing-location-data-of-thousands-of-innocent-people (last accessed: 18.07.2013)

King, N.J., Jessen, P.W. (2014) Smart metering systems and data sharing: why getting a smart meter should also mean getting strong information privacy controls to manage data sharing, *International Journal of Law and Information Technology*, pp. 1-39

Kleining, J., Mameli, P., Miller, S., Salane, D., Schwartz, A. (2011) Security and Privacy: Global standards for ethical identity management in contemporary liberal democratic states, *ANU E Press*

Klitou, D. (2014), Privacy invading technologies and privacy by design, Springer

Knigge, G. (2013) On presuming innocence, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 225-238

Knyrim, R., Trieb, G. (2011) Smart metering under EU data protection law, *International Data Privacy Law*, vol. 1, no. 2, pp. 121-128

Kokott, J., Sobotta, C. (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law*, vol. 3, no. 4, pp. 222-228

Koops, B.J. (2010), Law, Technology, and shifting power relations, *Berkeley Technology Law Journal*, vol. 25, no. 2, pp. 973-1035

Koops, B.J. (2013), Police investigations in Internet open sources: procedural-law issues, *Computer Law & Security Review*, vol. 29, no. 6, pp. 654-665

Korff, D. (2013) Note on European and International law on trans-national surveillance prepared for the Civil Liberties Committee of the European Parliament to assist the Committee in its enquires into USA and European States' surveillance, available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/note_korff_/note_korff_en.pdf (last accessed: 1.11.2013)

Korff, D. (2014) The rule of law on the internet and in the wider world, *Issue Paper published by the Council of Europe Commissioner for Human Rights*, available online at: https://wcd.coe.int/ViewDoc.jsp?id=2268589 (last accessed: 1.11.2014)

Kosta, E. (2013) The way to Luxemburg: National Court decisions on the compatibility of the data retention directive with the rights to privacy and data protection, *SCRIPTed*, vol. 10, no. 3, pp. 339-363

Kuneva, M. (2009), Keynote Speech at Roundtable on Online data collection, targeting and profiling, Brussels 31 March 2009, Speech/09/156, available online at: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (last accessed: 26.7.2016)

Landau, S. (2015) Control use of Data to Protect Privacy, *Science*, vol. 347, no. 6221, DOI: 10.1126/science.aaa4961

Lane, N.D. et al. (2010) A survey of mobile phone sensing, *IEEE Communications Magazine*, vol. 48, no. 9, pp. 140-150

Le Grand, G., Barrau, E. (2012), Prior checking, a forerunner to privacy impact assessments, in Wright, D., De Hert, P. (eds.), *Privacy Impact Assessment*, pp. 97-116

Leaver, T., Lloyd, C. (2015) Seeking transparency in locative media, in Wilken, R., Goggin, G. (eds.), *Locative media*, pp. 162-176

Leczykiewitz, D. (2013) Horizontal application of the Charter of Fundamental Rights, *European Law Review*, vol. 38, pp. 479-497

Lee, D. (2013) Boston bombing: How internet detectives got it very wrong, in *BBC News*, 19 April 2013, available online at: http://www.bbc.com/news/technology-22214511 (last accessed: 12.2.2016)

Leigh, I. (2005) More closely watching the spies: Three decades of experiences, at Born, H. et al. (eds.) *Who's watching the spies?: Establishing intelligence service accountability*, pp. 3-11

Lerner, J.I., Mulligan, D.K. (2008) Taking the long view on the fourth amendment: Stored records and the sanctity of the home, *Stanford Technology Law Review*, vol. 3, available online at: http://scholarship.law.berkeley.edu/facpubs/2501/ (last accessed: 12.2.2016)

Lisovich, M., Mulligan, D., Wicker, S. (2010) Inferring personal information from demand-response systems, *IEEE Security and Privacy*, pp. 11-20

Lo Schiavo, L., Delfanti, M., Fumagalli, E., Olivieri, V. (2013) Changing the Regulation for Regulating the Change - Innovation-driven regulatory developments in Italy: smart grids, smart metering and e-mobility, *Energy Policy*, vol. 57, pp. 506-517

Loader, I. (2002) Policing, securitization and democratization in Europe, *Criminology and Criminal Justice*, vol. 2, no. 2, pp. 125-153

Lynskey, O. (2014) Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order, *International and Comparative Law Quarterly,* vol. 63, no. 3, pp. 569-597

Lynskey, O. (2014) Deconstructing data protection: the "added-value" of a right to data protection in the EU legal order, *International and Comparative Law Quarterly,* vol. 63, no. 3, pp. 569-597

Lyon, D. (2003) Surveillance as social sorting: Computer codes and mobile bodies, in Lyon, D. (eds.) *Surveillance as social sorting: Privacy, risk and automated discrimination*, pp. 13-30

Lyon, D. (2007) Surveillance studies: An overview, Polity Press

Lyon, D., (2007) Surveillance, power and everyday life, in Mansell, R., Avgerou, C., Quah, D., Silverstone, R. (eds.), The Oxford handbook of Information and Communication technologies, available online at: http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199548798.001.0001/oxfordhb-9780199548798-e-019 (last accessed: 12.2.2016)

MacAskill, E., Borger, J., Hopkins, N., Davies, N., Ball, J. (2013) GCHQ taps fiber-optic cables for secret access to world's communications, *The Guardian* (21 June 2013), available online at: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (last accessed: 20.1.2014)

MacAskill, E., Borger, J., Hopkins, N., Davies, N., Ball, J. (2013) Mastering the internet: how GCHQ set out to spy on the world wide web, *The Guardian* (21 June 2013), available online at: http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet (last accessed: 2.11.2013)

Maras, M.H. (2009) From targeted to mass surveillance: Is the EU data retention directive a necessary measure or an unjustified threat to privacy, in Goold, B.J., Neyland, D. (eds.), *New directions in surveillance and privacy*, pp. 74-105

Maras, M.H. (2011) While the European Union was sleeping, the data retention directive was passed: The political consequences of mandatory data retention, *Hamburg Review of Social Sciences*, vol. 6, no. 2, pp. 1-30

Marquardt P., Verma A., Carter H., Traynor P. (2011) (Sp)iphone: decoding vibrations from nearby keyboards using mobile phone accelerometers, *Proceedings of the 18th ACM Conference on Computer and Communications Security*, pp. 551–562

Martinez-Perez, B., Torre-Diez, I., Lopez-Coronado, D. (2014) Privacy and security in mobile health apps: A review and recommendations, *Journal of Medicine Systems*, vol. 39, no. 181, doi:10.1007/s10916-014-0181-3

Marx, G. (2002), What is new about “New surveillance”? Classifying for change and continuity, *Surveillance and Society*, vol. 1, no. 1, pp. 9-29

Marx, G. (2006) Ethics of the New surveillance, *The information society: An international journal*, vol. 14, no. 3, pp. 171-185

Marx, G. (2013) The Public as Partner? Technology Can Make Us Auxiliaries as Well as Vigilantes, *Security and Privacy, IEEE*, vol. 11, no. 5, pp. 56-61

Mayer-Schoenberger, V. (1997) Generational development of data protection in Europe, in Agre, P.E., Rotenberg, M. (eds.), *Technology and Privacy: The new landscape*, pp. 219-238

Mc Bride, J. (1999), Proportionality and the European Court of Human Rights, in Ellis, E. (eds.), *The principle of proportionality in the laws of Europe*, pp. 23-36

McCcormack, D. (2013) Ex-FBI official claims organization can remotely activate the mic on Android phones to record user's conversations, in *Daily Mail*, 2 August 2013, available online at: http://www.dailymail.co.uk/news/article-2383892/Ex-FBI-official-claims-organization-remotely-activate-mic-Android-phones-record-users-conversations.html (last accessed: 12.2.2016)

McCullagh D., Broache, A. (2006), FBI taps cell phone mic as eavesdropping tool, *CNET News*, December 2006, available at: http://news.cnet.com/2100-1029-6140191.html (last accessed: 29.7.2016)

McDaniel, P. (2009) Security and privacy challenges in the smart grid, *IEEE Security and Privacy*, vol. 7, pp. 75-77

McKenna, E., Richardson, I., Thomson, M. (2012) Smart meter data: Balancing consumer privacy concerns with legitimate applications, *Energy Policy*, vol. 41, pp. 807-814

Michael, K., McNamee, A., Michael, M.G. (2006) The emerging ethics of humancentric GPS tracking and monitoring, in *Proceedings of the International Conference on Mobile Business*, pp. 34-42

Michael, K., McNamee, A., Michael, M.G., Tootell, H. (2006) Location-based intelligence - Modeling behavior in humans using GPS, Proceedings of IEEE International Symposium on Technology and Society, pp. 1-8

Mifsud Bonnici, J.P. (2007) Recent European Union developments on data protection … in the name of Islam or 'Combating terrorism', *Information & Communications Technology Law*, vol. 16, no. 2, pp. 161-175

Mifsud Bonnici, J.P. (2013), Exploring the non-absolute nature of the right to data protection, *International Review of Law, Computer and Technology*, vol. 28, no. 2, pp. 131-143

Mifsud Bonnici, J.P. (2014) Redefining the relationship between security, data retention and human rights, in Holzhacker, R., Luif, P. (eds.), *Freedom, security and justice in the European Union*, pp. 49-74

Milaj, J. (2015) Invalidation of the Data Retention Directive – Extending the proportionality test, *The Computer Law and Security Review*, vol. 31, no. 5

Milaj, J. (2015) Privacy, surveillance and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance, *International Review of Law, Computers and Technology*, DOI: 10.1080/13600869.2015.1076993

Milaj, J., Mifsud Bonnici, J.P. (2014) Unwitting subjects of surveillance and the presumption of innocence, *Computer Law & Security Review*, vol. 30, no. 4, pp. 419-428

Milaj, J., Mifsud Bonnici, J.P. (2016) Privacy Issues in the Use of Smart Meters—Law Enforcement Use of Smart Meter Data, in Beaulieu, A., de Wilde, J. and Scherpen, J. (eds.), *Smart Grids from a Global Perspective: Bridging Old and New Energy Systems*, pp. 179-196

Milaj, J., Mifsud Bonnici, J.P. (2016) Smart meters as non-purpose built surveillance tools, in Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (eds.), *Privacy Technologies and Policy,* pp. 81-95

Milaj, J., Kaiser, C. (2017) Retention of data in the new Anti-Money Laundering directive – 'need to know' versus 'nice to know', *International Data Privacy Law*, DOI:https://doi.org/10.1093/idpl/ipx002

Mills, E. (2012) Researchers find smart meters could reveal favourite TV shows, *CNet News*, available online at: http://news.cnet.com/8301-27080_3-57364883-245/researchers-find-smart-meters-could-reveal-favorite-tv-shows/ (last accessed: 27.04.2013)

Mitsilegas, V. (2015) The transformation of privacy in the area of pre-emptive surveillance, *Tilburg Law Review*, vol. 20, pp. 35-57

Mobbs, P. (2003), Privacy and Surveillance: How and when organisations and the state can monitor your actions, *GreenNet CSIR*, no. 3, available online at: http://www.internetrights.org.uk/briefings/irtb05-rev1-draft.pdf (last accessed: 17.6.2015)

Moonen, T. (2010), Special Investigation Techniques, Data Processing and Privacy Protection in the Jurisprudence of the European Court of Human Rights, *Pace Int'l L. Rev. Online Companion*, pp. 97-142

Morariu, M. (2009) How secure is to remain private? On the controversies of the European Data Retention directive, *Amsterdam Social Science*, vol. 1, no. 2, pp. 46-65

Moskovitch, R., et al. (2009) Identity theft, computers and behavioral biometrics, in *Proceedings of the IEEE International Conference on Intelligence and Security Informatics,* pp. 155–160

Munir, A.B., Yasin, S.H.M. (2004) Retention of communications data: a bumpy road ahead, *Journal of Computer & Information Law*, vol. 22, pp. 731-758

Mylonas, A. (2013) Security and privacy in ubiquitous computing: The smart mobile equipment case, *Technical report series (Athens University)*, no. 3, pp. 139-141

Mylonas, A., Kastania, A., Gritzalis, D. (2013) Delegate the smartphone user? Security awareness in smartphone platforms, *Computers and Security*, vol. 34, pp. 47-66

Mylonas, A., Meletiadis, V., Tsoumas, B., Mitrou, L., Gritzalis, D. (2012) Smartphone forensics: A proactive investigation scheme for evidence acquisition, in Gritzalis, D. et al. (eds.), *Information security and privacy research*, pp. 249-260

Naughton, M. (2011) How the presumption of innocence renders the innocent vulnerable to wrongful convictions, *Irish Journal of Legal Studies*, vol. 2, no. 1, pp. 40-54

Nelson, F. (2014) Every 73 seconds, police use snooping powers to access our personal records. Who'll rein them in?, *The Spectactor*, 11 October 2014, available online in: http://www.spectator.co.uk/2014/10/now-its-the-police-snooping-in-your-mobile-phone/ (last accessed: 24.2.2016)

Newell, B.C. (2011) Rethinking Reasonable Expectations of Privacy in Online Social Networks, *Richmond Journal of Law and Technology*, vol. 17, no. 4, pp. 1-62

Norris, C., Murakami Wood, D. (2009) Evidence, in *House of Lords, Selected Committee on the Constitution, Surveillance: Citizens and the State*, HL paper 18-II, second report of session 2008-2009, Volume II: Evidence

Nouwt, J. (2008) Reasonable expectation of geo-privacy?, *SCRIPT-ed – A Journal of Law, Technology and Society*, vol. 5, no. 2, pp. 375-403

Nowak, K. (2011) Vetting surplus information before it can lead to human right infringements, deliverable prepared for DETECTOR (Detection technologies, terrorism, ethics and human rights) FP7 project, available online at: http://www.google.nl/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CCgQFjAB&url=http%3A%2F%2Fwww.detecter.bham.ac.uk%2Fpdfs%2FD15.2_Vetting_Surplus_Information.doc&ei=gdtdVdi0FcG4UYbQgLgN&usg=AFQjCNEqL-D2U6fiHzZ5wUZ1iIsK2R9axQ&bvm=bv.93756505,d.d24, (last accessed: 21.5.2015)

O'Cleirigh, F. (2016) French intelligence 'could have prevented Paris attacks', in *Computer Weekly*, available online at: http://www.computerweekly.com/news/4500270121/French-intelligence-could-have-prevented-Paris-attacks (last accessed: 10.2.2016)

O'Malley, P. (2013) The politics of mass preventive justice, in Ashworth, A. et al. (eds.), *Prevention and the limits of the criminal law*, pp. 273-295

Ohm, P. (2010), The Argument Against Technology-Neutral Surveillance Laws, *Texas Law Review*, vol. 88, pp. 1685-1713

Ovey, C., White, R. (2002) European Convention on Human Rights, OUP, 3rd edition

Pallas, F. (2012) Beyond gut level – Some critical remarks on the German privacy approach to smart metering, in Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (eds.), *European data protection: Coming of age*, Springer, pp. 313-345

Palmer, M. (2011) TomTom sorry for selling driver data to police, in *Financial Times*, 28 April 2011, available online at: http://www.ft.com/cms/s/2/3f80e432-7199-11e0-9b7a-00144feabdc0.html#axzz45th62fsM (last accessed: 15.4.2016)

Patil, S., Patruni, B., Lu, H., Dunkerley, F., Fox, J., Potoglou, D., Robinson, N. (2015) Public Perception of Security and Privacy - Results of the comprehensive analysis of PACT's pan-European Survey, available online at: http://www.rand.org/pubs/research_reports/RR704.html (last accessed: 28.7.2016)

Patton, J.W. (2000) Protecting privacy in public? Surveillance technologies and the value of public places, *Ethics and Information Technology*, vol. 2, pp. 181-187

Phipps, C., Rawlinson, K. (2015) Paris attacks kill more than 120 people – as it happened, in *the Guardian,* 14 November 2015, available online at:

https://www.theguardian.com/world/live/2015/nov/13/shootings-reported-in-eastern-paris-live (last accessed: 2.8.2016)

Poullet, Y. (2006) EU data protection policy. The Directive 95/46/EC: Ten years after, *Computer Law and Security Review*, vol. 22, no. 3, pp. 206-217

Quinn, E.L. (2008) Privacy and the new energy infrastructure, *CEES Working Paper no. 09-0001*, pp. 41

Raab, C., Ball, K., Graham, S., Lyon, D., Murakami Wood, D., Norris, C. (2006) 'Report on the Surveillance Society' for the information Commissioner's Office, available online at: http://www.surveillance-studies.net/?page_id=3 (last accessed: 2.5.2013)

Raab, C.D, Wright, D. (2012), Surveillance: Extending the limits of Privacy impact assessment, in Wright and De Hert (eds.), *Privacy Impact Assessment*, pp. 363-383

Rawlinson, K. (2015) National emergency? Belgians respond to terror raids with cats, *The Guardian*, 22 November 2014, available online at: http://www.theguardian.com/world/2015/nov/22/national-emergency-belgians-respond-with-cats (last accessed: 8.2.2016)

Reeves, J. (2012) If you see something, say something: Lateral surveillance and the uses of responsibility, *Surveillance and Society*, vol. 10, no. 3, pp. 235-248

Reichert, C. (2015) Germany moves closer to data retention, in *ZDNet*, 19 October 2015, available online at: http://www.zdnet.com/article/germany-moves-closer-to-data-retention/ (last accessed: 11.2.2016)

Reidenberg, J.R. (2014) The data surveillance state in the United States and Europe, *Wake Forest Law Review*, vol. 49, pp. 583-608

Richards, N.M. (2013) The dangers of surveillance, *Harvard Law Review*, vol. 126, pp. 1934-1965

Rivers, J. (2002) A theory of Constitutional rights and the British Constitution, A translator's introduction, in Alexy, R., A theory of constitutional rights, OUP

Roach, K. (2010) The eroding distinction between intelligence and evidence in terrorism investigations, in McGarrity, N., Lynch, A., Williams, G. (eds.), *Counter-terrorism and beyond*, Routledge, pp. 48-68

Roberts, H., Palfrey, J. (2010) The EU Data Retention Directive in an era of internet surveillance, in Deibert, R. et al. (eds.) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, pp. 35 - 53

Rodota, S. (2006) The European Constitutional Model for Data Protection, available online at: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/rodota_/rodota_en.pdf (last accessed: 11.2.2016)

Rodota, S. (2009) Data protection as a fundamental right, in Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., Nouwt, S. (eds.), *Reinventing Data Protection?*, pp. 77-82

Roosendaal, A. (2013) Protecting individuals' rights in online contexts, Wolf Legal Publishers

Rosenbach, M., Poitras, L., Stark, H. (2013) iSpy: How the NSA Accesses Smartphone Data, in Der Spigel, 9 September 2013, available online at: http://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html (last accessed: 22.2.2016)

Rushin, S. (2011) The judicial response to mass police surveillance, *Journal of law, technology and policy*, no. 2, pp. 281-328

Savirimuthu, J. (2013) Smart meters and the information panopticon: beyond the rhetoric of compliance, *International Review of Law, Computes & Technology*, vol. 27, no. 1-2, pp. 161-186

Scassa, T. (2009) Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy, *Canadian Journal of Law and Technology*, vol. 7, no.2, pp. 193-220

Schneider, C.J., Trottier, D. (2012) The 2011 Vancouver riot and the role of Facebook in crowd-sourced policing, in *BC Studies*, no. 175, pp. 57-72

Schwartz, P. (1995) Privacy and participation: Personal information and public sector regulation in the United States, *Iowa law Review*, vol. 80, pp. 553-618

Scirocco, A. (2008) The Lisbon Treaty and the protection of personal data in the European Union, *Data Protection Review*, no. 5, available online at: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2008/08-09-19_Scirocco_Lisbontreaty_DP_EN.pdf (last accessed: 11.2.2016)

Shanon, V. (2016) Brussels attacks: What we know and what we don't know, in *New York Times*, 22 March 2016, available online at: http://www.nytimes.com/2016/03/23/world/europe/brussels-attacks-what-we-know-and-dont-know.html?_r=0 (last accessed: 2.8.2016)

Shiffman, J., Cooke, K. (2013) US directs agents to cover up programme used to investigate Americans, *Reuters* (5 August 2013), available online at: http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805 (last accessed: 10.2.2014)

Shklovski, I., et al. (2014) Leakiness and creepiness in app space: perceptions of privacy and mobile app use, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2347-2356

Sipior, J.C., Ward, B.T., Volonino, L. (2014) Privacy Concerns Associated with Smartphone Use, *Journal of Internet Commerce*, vol. 13, no. 3-4, pp. 177-193

Skog, I., Handel, P., (2009) In-car positioning and navigation technologies – A survey, in *IEEE Transactions on Intelligent Transportation Systems*, vol. 10, no. 1, pp. 4-20

Van der Sloot, B., van der (2014) Privacy in the Post-NSA Era: Time for a Fundamental Revision?, JIPITEC, vol. 5, n. 2, available online at: https://www.jipitec.eu/issues/jipitec-5-1-2014/3901 (last accessed: 12.4.2016)

Solove, D. (2011) Nothing to Hide: The False Tradeoff Between Privacy and Security, Yale University Press

Sorell, T. (2011) Preventive policing, surveillance, and European counter-terrorism, *Criminal Justice Ethics*, vol. 30, no. 1, pp. 1-22

Spaventa, E. (2014) Fundamental Rights in the European Union, in Barnard, C., Peers, S. (eds.), *European Union Law*, pp. 226-254

Stamp, G. (2011) English riots: Social media were "force for good", *BBC News*, 15 September 2011, available online at: http://www.bbc.com/news/uk-politics-14931010 (last accessed: 24.3.2016)

Starbird, K., Maddock, J., Orand, M., Achternam, P., Mason, R.M. (2014) Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing, *iConference 2014 proceedings*, available online at: https://hdl.handle.net/2142/47257 (last accessed: 24.3.2016)

Statista (2016) Statistics on the Number of free and paid mobile app store downloads worldwide from 2011 to 2017, available online at: http://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-app-store-downloads/ (last accessed: 23.2.2016)

Stupp, C. (2016) Commission plans export controls for surveillance technology, available online at: https://www.euractiv.com/section/trade-society/news/technology-companies-face-export-hurdles-under-draft-eu-rules/ (last accessed: 2.8.2016)

Subrahmanyan, P.A. (2005) Network security architecture for demand response/sensor networks, Report for the California Energy Commission, Public Interest Energy Research Group, available online at: http://www.law.berkeley.edu/files/demand_response_CEC.pdf (last accessed: 15.4.2015)

Svedsen, A.D.M. (2011) On 'a Continuum with expansion'? Intelligence co-operation in Europe in the early twenty-first century, *Journal of Contemporary European Research*, vol. 7, no. 4, pp. 520-538

Tadros, V. (2007) Rethinking the presumption of innocence, *Criminal Law and Philosophy*, vol. 1, pp. 193-213

Taipale, K.A. (2005) The trusted systems problem: Security envelopes, statistical threat analysis, and the presumption of innocence, *IEEE Intelligent Systems*, vol. 20, no. 5, pp. 80-82

Tanner, A. (2014), What stays in Vegas, Public Affairs

Taylor, N. (2001) State surveillance and the right to privacy, in *Surveillance and Society*, vol. 1, no. 1, pp. 66-85

Taylor, N. (2003) Policing, privacy and proportionality, *European Human Rights Law Review, Supplement (Special issue: Privacy 2003)*, pp. 86-100

Taylor, N. (2011) A conceptual legal framework for privacy, accountability and transparency in visual surveillance systems, *Surveillance and Society*, vol. 8, no. 4, pp. 455-470

Theoharidou, M., Mylonas, A., Gritzalis, D. (2012) A risk assessment method for smartphones, in Gritzlis, D. et al. (eds.) *Information security and privacy research*, pp. 443-456

Thing V.L., Ng K.Y., Chang E.C. (2010) Live memory forensics of mobile phones, *Digital Investigation: The International Journal of Digital Forensics & Incident Response*, vol. 7, (supplement), pp. 74–82

Thommesen, J., Andersen, H.B. (2009) Privacy implications of surveillance systems, available online at: http://orbit.dtu.dk/fedora/objects/orbit:56150/datastreams/file_4010841/content (last accessed: 6.5.2013)

Timberg, C., Miller, G. (2014) FBI blasts Apple, Google for blasting FBI out of phones, in The *Washington Post*, 25 September 2014, available online at: https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html (last accessed: 15.2.2016)

Togias, S. (2011) The right in confidentiality and integrity of information technology systems according to the German Federal Constitutional Court: "Old wine in new bottles?", in Kanellopoullou, M.M. (eds.), *An information law for the 21st century*, pp. 530-540

Töllborg, D. (1995) Undercover in Sweden: The Swedish security police and their modus operandi, in Fijnaut, C., Marx, G. (eds.) *Undercover: Police Surveillance in Comparative Perspective*, pp. 248-268

Tomilson, E.A. (1993) The saga of wiretapping in France: What it tells us about the French criminal justice system, *Louisiana Law Review*, vol. 53, no. 4, p. 1091-1152

Trechsel, S. (2006) The right to be presumed innocent, in Trechsel, S., Summers, S. (eds.), *Human rights in criminal proceedings*, pp. 153-191

Tridimas, T. (1999), Proportionality in European Community law: Searching for the appropriate standard of scrutiny, in Ellis, E. (eds.), *The principle of proportionality in the laws of Europe*, pp. 65-84

Troncoso Reigada, A. (2012) The principle of proportionality and the fundamental right to personal data protection: The biometric data processing, *Lex Electronica*, vol. 17, no. 2, pp. 1-44

Tropjan, C. (2014) The next data privacy battle may be waged inside your car, *The New York Times*, 10 January 2014, available online at: http://www.nytimes.com/2014/01/11/business/the-next-privacy-battle-may-be-waged-inside-your-car.html?_r=0 (last accessed: 12.4.2016)

Tsai, J.Y., Gage Kelley, P., Faith Cranon, L., Sadeh, N. (2010) Location-sharing technologies: Privacy risks and controls, *A Journal of Law and Policy for the Information Society*, vol. 6, no. 2, pp. 119-317

Ulvang, M. (2013) Presumption of innocence versus a principle of fairness, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 205-224

Vatney, M. (2006) The justifiability of state surveillance of internet communications as an e-security mechanism, available online at: http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/117_Paper.pdf (last accessed: 17.02.2015)

Vaz, P., Bruno, F. (2003) Types of self-surveillance: from abnormality to individuals 'at risk', in *Surveillance & Society*, vol. 1, no. 3, pp. 272-291

Verhey, L. (2014) Privacy in the Dutch Constitution: a dead letter?, in Hijmans, H., Kranenborg, H. (eds.), *Data protection anno 2014: How to restore trust?,* pp. 69-81

Vervaele, J.A.E. (2005) Terrorism and information sharing, *Utrecht Law Review*, vol. 1, no. 1, pp. 1-27

Wahlgren, P. (2000), On the future of legal science, *Scandinavian Studies in Law*, vol. 40, pp. 515-525

Wainright, R. (2007) Father and son stick to guns to prove radar wrong, *Sidney Morning Herald*, 12 March 2007, available online at: http://www.smh.com.au/news/national/father-and-son-stick-to-guns-to-prove-radar-wrong/2007/03/11/1173548023012.html (last accessed: 21.4.2016)

Waters, N. (2012), Privacy impact assessment – Great potential not often realized, in Wright, D., De Hert, P. (eds.), *Privacy Impact Assessment*, pp. 149-160

Watney, M. (2008) Understanding electronic surveillance as an investigatory method in conducting criminal investigations on the internet, available online at: http://www.isrcl.org/Papers/2008/Watney.pdf (last accessed: 27.1.2014)

Weigend, T. (2013) There is only one presumption of innocence, *Netherlands Journal of Legal Philosophy*, vol. 42, no. 3, pp. 193-204

Weiss, M., Helfenstein, A., Mattern, F., Staake, T. (2012) Leveraging smart meter data to recognize home appliances, in *Proceedings of IEEE Pervasive Computing and Communication PerCom*, pp. 190-197

White, R.C.A., Ovey, C. (2010) The European Convention on Human Rights, Oxford University Press, 5th edition

Wicker, S.B. (2011) Cellular telephony and the question of privacy, *Communications of the ACM*, vol. 54, no. 7, pp. 88-98

Wiebe, A. (2008) The new fundamental right to IT security – first evaluation and comparative view at the U.S., *Datenschutz und Datenschicherheit*, vol. 32, no. 11, pp. 713-716

Wigan, M., Clarke, R. (2006) Social impacts of transport surveillance, in *Prometheus: Critical studies in Innovation*, vol. 24, no. 4, pp. 389-403

Wright, D. (2012), The state of art in privacy impact assessment, *Computer Law and Security Review*, vol. 28, pp. 54-61

Wright, D. et al. (2010) Sorting out smart surveillance, *Computer law & Security review*, vol. 26, pp. 343-354

Wright, D. et al. (2014) SAPIENT Deliverable 4.4: A guide to surveillance impact assessment – How to identify and prioritise risks arising from surveillance systems, available online at: http://www.sapientproject.eu/D4.4%20-%20SIA%20Manual%20(submitted%2001%20August%202014).pdf (last accessed: 11.6.2015)

Wright, D., De Hert, P. (2012) Introduction to Privacy Impact Assessment, in Wright, D., De Hert, P. (eds.), *Privacy Impact Assessment*, pp. 3-32

Wright, D., Finn, R., Rodrigues, R. (2013) A comparative analysis of Privacy Impact Assessment in six countries, *Journal of Contemporary European Research*, vol. 9, no. 1, pp. 160-180

Wright, D., Raab, C.D. (2012) Constructing a surveillance impact assessment, *Computer Law and Security review*, vol. 28, pp. 613-626

Wright, D., Raab, C.D. (2014) Privacy principles, risks and harms, *International Review of Law, Computers and Technology*, vol. 28, no. 3, pp. 277-298

Wynn, G. (2010) Privacy concerns challenge smart grid rollout, Reuters 25 June 2010, available online at: http://www.reuters.com/article/2010/06/25/energy-smart-idUSLDE65N2CI20100625 (last accessed: 13.5.2015)

Young, S. (2013) A wireless brain-computer interface, available online in: http://www.technologyreview.com/news/512161/a-wireless-brain-computer-interface/ (last accessed: 24.04.2013)

Young, S. (2013) A wireless brain-computer interface, available online in: http://www.technologyreview.com/news/512161/a-wireless-brain-computer-interface/ (last accessed: 24.04.2013)

Zachman, J. (1987) A framework for information systems architecture, *IBM Systems Journal*, vol. 26, no. 3, pp. 276–292

Zallone, R. (2014) Here, there and everywhere: Mobility data in the EU (Help needed: Where is privacy?), *Santa Clara High Tech. L.J.*, vol. 30, no. 1, pp. 57-88

Zavesnik, A. (2013) Blurring the line between law enforcement and intelligence: Shaping the gaze of surveillance?, *Journal of contemporary European research*, vol. 9, no. 1, pp. 181-202

Zeadalli, S., Pathan, A.-S., Alcaraz, C., Badra, M. (2013) Towards privacy protection in smart grid, *Wireless Personal Communication*s, vol. 73, pp. 23-50

Zhao, Y. (2000) Mobile phone location determination and its impact on intelligent transportation systems, in *IEEE*, vol. 1, no. 1, pp. 55-64

Zhou, L., Xu, F.-Y., Ma, Y.-N. (2010) Impact of smart metering on energy efficiency, *Proceedings of ICMLC 2010 International conference*, vol. 6, pp. 3213-3218

Legal sources

COM(2017) 10 final Proposal for a Regulation of the European parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC

Convention for the protection of individuals with regard to automatic processing of personal data, No. 108, 28 January 1981

Convention on mutual assistance in criminal matters between the Member States of the European Union, OJ C 197

Datenschutzgesetz 2000, Bundesgesetz über den Schutz personenbezogener Daten

Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, OJ L 141, 5.6.2015

Directive 2016/681/EU of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4.5.2016

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002

Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments, OJ L 135, 30.4.2004

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006

Directive 2006/32/EC of the European Parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC, OJ L 114, 27.4.2006

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009

Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, OJ L 211, 14.8.2009

Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, OJ L 211, 14.8.2009

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014

Directive 2016/343/EU of the European Parliament and of the Council of 9 March 2016 on the strengthening of certain aspects of the presumption of innocence and of the right to be present at the trial in criminal proceedings, OJ L 65, 11.3.2016

Directive 2016/680/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent

authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23.11.1995

International Covenant on Civil and Political Rights (ICCPR) adopted by the United Nations General Assembly on 16 December 1966

Parliamentary Assembly of the Council of Europe (2015) Recommendation 2067(2015) on Mass surveillance

Rec(2001)10 of the Committee of Ministers to the Member States on the European code of police ethics

Rec(2005)10 of the Committee of Ministers to the Member States on “special investigation techniques” in relation to serious crimes including acts of terrorism

Rec(2007)1 of the Committee of Ministers to the Member States on co-operation against terrorism between the Council of Europe and its Member States, and the International Criminal Police Organisation (ICPO - Interpol)

Rec(2007)16 of the Committee of Ministers to the Member States on measures to promote the public service value of the Internet

Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling

Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling

Rec(2012)3 of the Committee of Ministers to the Member States on the protection of human rights with regards to search engines

Rec(2012)4 of the Committee of Ministers to the Member States on the protection of human rights with regard to social networking services

Recommendation No. R (2002) 9 on the protection of personal data collected and processed for insurance purposes

Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics

Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing

Recommendation No. R (86) 1 on the protection of personal data used for social security purposes

Recommendation No. R (87) 15 regulating the use of personal data in the police sector

Recommendation No. R (89) 2 on the protection of personal data used for employment purposes

Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations

Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies

Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services

Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services

Recommendation No. R (97) 18 concerning the protection of personal data collected and processed for statistical purposes

Recommendation No. R (97) 5 on the protection of medical data

Recommendation No. R (99) 5 on the protection of privacy on the Internet

Regulation 1049/2001/EC of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001

Regulation 1987/2006/EC of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28.12.2006

Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001

Regulation 767/2008/EC of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008

Regulation 1077/2011/EU of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011

Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016

Regulation 2016/794/EC of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016

Regulation 603/2013/EU of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180, 29.6.2013

UK Data retention and Investigatory powers act 2014

Council Regulation 2725/2000/EC of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000

Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 063, 6.3.2002

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004

Council Regulation 2252/2004/EC of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385/1, 29.12.2004

Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record, OJ L 322, 9.12.2005

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L 210, 6.8.2008

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008

Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L 350, 30.12.2008

Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93, 7.4.2009

Commission Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems, OJ L 73, 13.3.2012

Commission Recommendation 2014/724/EU of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, OJ L 300, 18.10.2014

Other documents

Article 29 Data Protection Working Party (2007) Opinion 4/2007 on the Concept of personal data, adopted on 20 June 2007

Article 29 Data Protection Working Party (2008) Opinion 1/2008 on Data protection issues related to search engines, adopted on 4 April 2008

Article 29 Data Protection Working Party (2011) Opinion 12/2011 on Smart Metering, adopted on 4 April 2011

Article 29 Data Protection Working Party (2011) Opinion 13/2011 on Geolocation services on smart mobile devices, adopted on 16 May 2011

Article 29 Data Protection Working Party (2013) Opinion 3/2013 on Purpose limitation, adopted on 2 April 2013

Article 29 Data Protection Working Party (2013) Opinion 4/2013 on the Data protection impact assessment template for smart grid and smart metering systems prepared by Expert Group 2 of the Commission´s Smart Grid Task Force, adopted on 22 April 2013

Article 29 Data Protection Working Party (2015) Opinion 3/2015 on the Draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, adopted on 1 December 2015

Article 29 Data Protection Working Party (2009) The future of privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009

Article 29 Working Party (2013) Opinion 2/2013 on Apps on smart devices, adopted on 27 February 2013

BEUC et al. (2011) Essential regulatory requirements and recommendations for data handling, data safety, and consumer protection, Recommendation to the European Commission, 5 December 2011, available online at: https://ec.europa.eu/energy/sites/ener/files/documents/Recommendations%20regulatory%20requirements%20v1.pdf (last accessed: 22.11.2016)

CBP (2011) Official investigation by the CBP into the processing of geolocation data by TomTom N.V., public version available online at: https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_pb_20120112_investigation-tomtom.pdf (last accessed: 13.4.2016)

Charter of Fundamental Rights of the European Union, OJ C 364/1, 18.12.2000

CNIL (2015) Privacy Impact Assessment: Methodology (how to carry out a PIA), available online at: http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf (last accessed: 27.10.2016)

COM(2005)172, on compliance with the Charter of Fundamental Rights, Brussels, 27.4.2005

COM(2005)184 final, Communication from the Commission to the Council and the European Parliament of 10 May 2005 – The Hague Programme: ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice, OJ C 236, 24.9.2005

COM(2005)597, Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, Brussels, 24.11.2005

COM(2006)174 final, Green Paper presented by the Commission, The presumption of innocence, Brussels 26.4.2006

COM(2010)609 final, Communication from the Commission to the EP, the Council, the ECOSOC and the CoR – A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010

COM(2010)673 final, Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, Brussels, 22.11.2010

COM(2011)255 final, Evaluation Report on the Data Retention Directive, Brussels, 18.4.2011

COM(2012)012 final, Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29(2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

COM(2012)9 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century, Brussels, 25.1.2012

COM(2015)185 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security, Strasbourg, 28.4.2015

Commission staff working document (2014) Cost-benefit analyses & state of play of smart metering deployment in the EU-27 - Accompanying the document Report from the Commission Benchmarking smart metering deployment in the EU-27 with a focus on electricity /* SWD/2014/0189 final */

Committee of Ministers of the CoE, Guidelines on human rights and the fight against terrorism, 11 July 2002

Committee on Civil Liberties, Justice and Home Affairs (2013) Working document 1, on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights, Rapporteur: Claude

Moraes, available online at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf (last accessed: 20.12.2013)

Committee on legal affairs and human rights (2015) Explanatory memorandum on the Parliamentary Assembly of the Council of Europe draft Resolution and draft Report on Mass Surveillance prepared by Mr. Pieter Omtzigt, rapporteur, available online at: http://assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=21583&lang=en (last accessed: 28.4.2015)

Consultative Committee on the protection of individuals with regards to automatic processing of personal data (2012) (T-PD)

Council of Europe (2002) Report on the impact of data protection principles on judicial data in criminal matters including in the framework of judicial co-operation in criminal matters

Council of Europe (2015) Declaration of the Committee of Ministers on ICANN, human rights and the rule of law, 3 June 2015

Council of Europe Commissioner for HR (2015), Democratic and effective oversight of national security services, issue paper, available online at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680487770 (last accessed: 21.11.2016)

Council of Europe, Declaration of the Committee of Ministers on risks to fundamental rights stemming from digital tracking and other surveillance technologies, 11 June 2013

Council of the European Union (2008) Council conclusions on a concerted work strategy and practical measures against cybercrime, 2987th Justice and Home Affairs Council meeting, 27-28 November 2008

Council of the European Union 9009/14 LIMITE, Information note from the general Secretariat of the Council to the Permanent Representatives Committee/Council, Brussels, 5 May 2014, available online at: http://www.statewatch.org/news/2014/may/eu-council-note-data-retention-judgment-9009-14.pdf (last accessed: 21.11.2016)

Danish Ministry of Justice (2014) Legal analyses on the CJEU ruling on the Data Retention Directive, available (in Danish) online at: http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf (last accessed: 22.11.2016)

Dutch government (2014) Reaction on national data retention laws after the CJEU ruling on the Data Retention Directive, available online at: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/11/19/tk-reactie-van-het-kabinet-naar-aanleiding-van-de-ongeldigverklaring-van-de-richtlijn-dataretentie.html (last accessed: 21.11.2016)

EDPS (2011) Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)

EDPS (2012) Opinion of the European Data Protection Supervisor on the Commission Recommendation on preparations for the roll-out of smart metering systems

EDPS (2015) Guidelines on the protection of personal data in mobile devices used by the European Institutions

ENISA (2015) Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics, available online at: https://www.enisa.europa.eu/publications/big-data-protection (last accessed: 22.11.2016)

Eurobarometer 71, available online at: http://ec.europa.eu/public_opinion/archives/eb/eb71/eb71_std_part1.pdf (last accessed: 22.11.2016)

European Commission (2011) A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the Smart Meter, available online at: https://ec.europa.eu/energy/sites/ener/files/documents/2011_10_smart_meter_funtionalities_report_full.pdf (last accessed: 22.11.2016)

European Commission (2012) Ethical and regulatory challenges to science and research policy at global level, Directorate General for research and innovation, available online at: http://ec.europa.eu/research/science-society/document_library/pdf_06/ethical-and-regulatory-challenges-042012_en.pdf (last accessed: 22.11.2016)

European Commission (2015) European Commission statement on national data retention laws, 16 September 2015, Statement/15/5654

European Commission (2016) Joint Statement on the final adoption of the new EU rules for personal data protection, 14 April 2016, available online at: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm (last accessed:1.5.2016)

European Commission for Democracy through Law, Report on the democratic oversight of the security services, study no. 388/2006

European Commission, Smart Grid Task Force 2012-2014, Expert Group 2, Data protection impact assessment template for smart grid and smart metering systems, available online at: https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf (last accessed: 4.1.2016)

European Parliament (2014) Report on the US NSA surveillance programmes, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Homme Affairs (2013/2188(INI)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, no. 139, 21.02.2014

European Parliament (2014) Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs

European Parliament (2015) Resolution of 12 March 2015 on the Annual Report on Human Rights and Democracy in the World 2013 and the European Union's policy on the matter

European Parliament (2015) Resolution of 29 October 2015 on the follow-up to the European Parliament resolution of 12 March 2014 on the electronic mass surveillance of EU citizens

European Parliament (2015) Resolution of 8 September 2015 on Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries

Human Rights Council Report (A/HRC/17/31) Guiding principles on business and human rights – Implementing the United Nations "Protect, Respect and Remedy" framework

ICO (2014) Conducting privacy impact assessments code of practice, available online at: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (last accessed: 27.10.2016)

Initiative taken by the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden with a view to adopting a directive of the European Parliament and of the Council regarding the European investigation order in criminal matters, available online at: http://ec.europa.eu/justice/news/intro/doc/comment_2010_08_24_en.pdf (last accessed: 22.11.2016)

Leeds City Council Legal Services (2000) Guiding document to the UK Regulation of Investigatory Powers Acts 2000, available online at: http://www.leeds.gov.uk/docs/RIPA%20Guidance%20and%20Procedure%20-%20May%202013.pdf (last accessed: 30.03.2015)

OECD (2014) Measuring the digital economy: A new perspective, available online at: http://www.oecd.org/sti/measuring-the-digital-economy-9789264221796-en.htm (last accessed: 13.5.2015)

Office of the United Nations High Commissioner for Human Rights (2014) The right to privacy in the digital age, 30 June 2014

PACE Report on Mass surveillance (provisional version) from rapporteur P. Omtzigt, available online at: http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2 (last accessed 29.1.2015)

Parliamentary Assembly of the Council of Europe (2015) Resolution 2045(2015) on Mass surveillance

Praesidium of the European Convention (2007) Explanations relating to the Charter of Fundamental Rights, OJ C 303/17, 14.2.2007

Resolution 17/4 adopted by the Human Rights Council on Human rights and transnational corporations and other business enterprises, 6.7.2011

Resolution 2045(2015) of the Parliamentary Assembly of the Council of Europe on Mass Surveillance, 21.04.2015

Smart Grid Coordination Group (2014) Document for the M/490 Mandate Smart Grid Information society, available online at: ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf (last accessed: 29.4.2015)

Tampere European Council Conclusions, available online at: http://www.europarl.europa.eu/summits/tam_en.htm (last accessed: 29.4.2015)

The European Council internal security strategy for the European Union - Towards a European Security Model, Brussels, 23 February 2010

The Stockholm Programme — An open and secure Europe serving and protecting citizens, OJ C 115, 4.5.2010

UK Smart metering implementation programme PIA 2012, available online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43044/7226-sm-privacy-ia.pdf (last accessed: 4.1.2016)

UN General Assembly Report of the Special Rapporteur Ben Emmerson (2014) on the Promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397, 23 September 2014

UN High Representative on Human Rights (2016) Statement on the Apple-FBI case, 4 March 2016, available online at: http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E (last accessed: 11.3.2016)

UN OHCHR (2014) The right to privacy in the digital age - Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014

Case law

CJEU

Case 29/69 *Stauder* [1969] ECR 419

Case 11/70 *Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide* [1970] ECR1125

Case 4/73 *Nold* [1974] ECR 491

Case C-265/87 *Schraeder HS Kraftfutter GmbH & Co KG v. Hauptzollamt Gronau* [1989] ECR 2237

Case C-331/88 *The Queen v. Minister of Agriculture, Fisheries and Food and Secretary of State for Health, ex parte: Fedesa et al.* [1990] ECR I-4023

Case C-260/89 *Elliniki Radiophonia Tileorassi AE (ERT) v. Dimotiki Etairia Pliroforissis* [1991] ECR I-2925

Case C-159/90 *The Protection of Unborn Children Ireland Ltd v. Stephen Grogan and others* [1991] ECR I-04685, Opinion of AG van Gerven

Case C-84/94 *United Kingdom v. Council* [1996] ECR I-5755

Opinion 2/94 on Accession by the Community to the ECHR [1996] ECR I-1759

Case C-60/00 *Carpenter* [2002] ECR I-6279

Case C-112/00 *Eugene Schmidberger, Internationale Transporte und Planzuge v. Austria* [2003] ECR I-5659

Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and others* [2003] ECR I-04989

Case C-101/01 *Lindqvist* [2003] ECR I-12971

Case C-491/01 *The Queen v. Secretary of State for Health, ex parte British American Tobacco (Investments) Ltd and Imperial Tobacco Ltd* [2002] ECR I-11453

Joined cases C-453/03, C-11/04, C-12/04 and C-194/04 *ABNA Ltd et al. v. Secretary of Health et al.* ECR I-10423

Case C-180/04 *Vassallo v. Azienda Ospedaliera Ospedale San Martino di Genova e Cliniche Universitarie Convenzionate* [2006] ECR I-7251

Case T-194/04 *Bavarian Lager v. Commission* [2007] ECR II-04523

Joined Cases C-317/04 and 318/04 *European Parliament v. Council and Commission* [2006] ECR I-4721

Joined cases C-402/05P and C-415/05P *Kadi and Al Barakaat v. Council* [2008] ECR I-6351

Case C-275/06 *Promusicae* [2008] ECR I-00271

Case C-301/06 *Ireland v. Parliament and Council* [2009] ECR I-00593

Case C-524/06 *Heinz Huber v. Bundesrepublik Deutschland* [2008] ECR I-09705, Opinion of AG Maduro

Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-09831

Case C-28/08P *Commission v. Bavarian Lager* [2010] ECR I-06055

Case C-543/09 *Deutsche Telecom* [2011] ECR I-03441

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, Opinion of AG Sharpstone

Case C-70/10 *Scarlet Extended* [2011] ECR I-11959, Opinion of AG Cruz Villalon

Case C-617/10 *Aklagaren v. Hans Akerberg Fransson* EU:C:2013:280

Case C-300/11 *ZZ v. Secretary of State for the Home Department* EU:C:2013:363

Case C-131/12 *Google Spain* EU:C:2014:317

Case C-131/12 *Google Spain* EU:C:2014:317, Opinion of AG Costeja Gonzalez

Case C-291/12 *Schwarz v. Stadt Bochum* EU:C:2013:670

Joint Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* EU:C:2014:238

Joint cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* EU:C:2014:238, Opinion of AG Cruz Villalon

Case C-390/12 *Pfleger et al.* EU:C:2014:281

Case C-473/12 *Institut professionnel des agents immobiliers (IPI) v. Geoffrey Engelbert, Immo 9 SPRL, Gregory Francotte* EU:C:2013:715

Case C-212/13 *Rynes* EU:C:2014:2428

Opinion 2/13 of the CJEU on the accession of the EU in the ECHR EU:C: 2014:2454

Case C-362/14 *Schrems v. Data protection Commissioner* EU:C:2015:650

Joined cases C-203/15 and C-698/15 *Tele2 Sverige* EU:C:2016:970

ECtHR

A. v. France, ECHR application no. 14838/89, 23 November 1993

Adolf v. Austria, ECHR application no. 8269/78, 26 March 1982

Airey v. Ireland, ECHR application no. 6289/73, 9 October 1979

Allenet de Ribemont, ECHR application no. 15175/89, 10 February 1995

Amann v. Switzerland, ECHR application no. 27798/95, 16 February 2000

Association "21 December 1989"and Others v. Romania, ECHR application no. 33810/07 and 18817/08, 24 May 2011

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, ECHR application no. 62540/00, 28 June 2007

B.B. v. France, ECHR application no. 5335/06, 17 December 2009

Barbera, Messegue and Jabardo v. Spain, ECHR application no. 100588/83, 10589/83 and 10590/83, 6 December 1988

Bernh Larsen Holding AS and others v. Norway, ECHR application no. 24117/08, 14 March 2013

Botta v. Italy, ECHR application no. 21439/93, 24 February 1998

Brusco v. France, ECHR application no. 1466/07, 14 October 2010

Copland v. The United Kingdom, ECHR application no. 62617/00, 3 April 2007

Cossey v. The United Kingdom, ECHR application no. 10843/84, 27 September 1990

Deweer v. Belgium, ECHR application no. 6903/75, 27 February 1980

Drakšas v. Lithuania, ECHR application no. 36662/04, 31 July 2012

Dudgeon v. The United Kingdom, ECHR application no. 7525/76, 24 February 1983

Esbester v. the United Kingdom, ECHR application no. 18601/91, Commission decision of 2 April 1993

Foti and others v. Italy, ECHR application no. 7604/76, 10 December 1982

Friedl v. Austria, ECHR application no. 15225/89, 31 January 1995

Gaskin v. The United Kingdom, ECHR application no. 10454/83, 7 July 1989

Halford v. The United Kingdom, ECHR application no. 20605/92, 25 June 1997

Handyside v. United Kingdom, ECHR application no. 5493/72, 7 December 1976

Heaney and McGuinness v. Ireland, ECHR application no. 34720/97, 21 December 2000

Huvig v. France, ECHR application no. 11105/84, 24 April 1990

Iordachi and others v. Moldova, ECHR application no. 25198/02, 24 September 2009

Keegan v. Ireland, ECHR application 16969/90, 26 May 1994

Kennedy v. the United Kingdom, ECHR application no. 26839/05, 18 May 2010

Khan v. The United Kingdom, ECHR application no. 35394/97, 12 May 2000

Khelili v. Sweden, ECHR application no. 16188/07, 18 October 2011

Klass v. Germany, ECHR application no. 5029/71, 6 September 1978

Kopp v. Switzerland, ECHR application no. 23224/94, 25 March 1998

Kruslin v. France, ECHR application no. 11801/85, 24 April 1990

Lambert v. France, ECHR application no. 23618/94, 24 August 1998

Leander v. Sweden, ECHR application no. 9248/81, 26 March 1987

Liberty and Others v. The United Kingdom, ECHR application no. 58243/00, 1 July 2008

Ludi v. Switzerlands, ECHR application no. 12433/86, 15 June 1992

M.K. v. France, ECHR application 19522/09, 18 April 2013

M.M. v. The Netherlands, ECHR application no. 39339/98, 8 April 2003

M.S. v. Sweden, ECHR application 20837/92, 27 August 1997

Malone v. The United Kingdom, ECHR application no. 8691/79, 2 August 1984

Marckx v. Belgium, ECHR application no. 6833/74, 13 June 1979

Matheron v. France, ECHR application no. 57752/00, 29 March 2005

Murray v. The United Kingdom, ECHR application no. 18731/91, 8 February 1996

Niemietz v. Germany, ECHR application no. 13710/88, 16 December 1992

P.G. & J.H. v. The United Kingdom, ECHR application no. 44787/98, 25 September 2001

Peck v. The United Kingdom, ECHR application no. 44647/98, 28 January 2003

Perry v The United Kingdom, ECHR application no. 63673/00, 17 July 2003

Popescu v. Romania (no. 2), ECHR application no. 71525/01, 26 April 2007

Pretty v. The United Kingdom, ECHR application no. 2346/02, 29 April 2002

Rees v. The United Kingdom, ECHR application no. 9532/81, 17 October 1986

Rotaru v. Romania, ECHR application no. 28341/95, 4 May 2000

Rushiti v. Austria, ECHR application no. 28389/95, 21 June 2000

S. and Marper v. The United Kingdom, ECHR application no. 30562/04 and 30566/04, 4 December 2008

Salduz v. Turkey, ECHR application no. 36391/02, 27 November 2008

Saunders v. UK, ECHR application no 19187/91, 17 December 1996

Sekanina v. Austria, application no. 13126/87, 25 August 1993

Shimovolos v. Russia, ECHR application 30194/09, 28 November 2011

Soering v. The United Kingdom, ECHR application no. 14038/88, 7 July 1989

Tyrer v. The United Kingdom, ECHR application no. 5856/72, 25 April 1978

Uzun v. Germany, ECHR application no. 35623/05, 2 September 2010

Van Vondel v. The Netherlands, ECHR application no. 38258/03, 25 October 2007

Von Hannover v. Germany, ECHR application no. 59320/00, 24 June 2004

Weber and Saravia v. Germany, ECHR application no. 54934/00, 29 June 2006

X and Y v. the Netherlands, ECHR application no. 8978/80, 26 March 1985

Z. v. Finland, ECHR application no. 22009/93, 25 February 1997

Zakharov v. Russia, ECHR application no. 47143/06, 4 December 2015

National

Arrêt no. 84/2015 du 11 juin 2015

BVerfG, NJW 2008, 1 BvR 370/07

Katz v. United States 389 U.S. 347 (1967)

Olmstead v. United States, 277 U.S. 438 (1928)

HR 5 September 2006 ECLI:NL:HR:2006:AV4149

PHR 5 September 2006 ECLI:NL:PHR:2006:AV4122

PHR 5 September 2006 ECLI:NL:PHR:2006:AV4144

RBDHA 11 March 2015 ECLI:NL:RBDHA:2015:2498

RBHAA 15 September 2010 ECLI:NL:RBHAA:2010:BO2789

RBZLY 6 May 2010 ECLI:NL:RBZLY:2010:BM3601

RBZUT 25 February 2011 ECLI:NL:RBZUT:2011:BP5729

Samenvatting

De nieuwe en geavanceerde technologie die we bezitten en dagelijks gebruiken (bijvoorbeeld slimme meters, smartphones, GPS apparaten etc.) is in staat om data van onze bezigheden en interesses stelselmatig te verzamelen en op te slaan. De inzet van deze technologie door wethandhavingsautoriteiten voor toezichtdoeleinden maakt hun werk efficiënter en faciliteert het in verscheidene opzichten: logistiek, technisch, economisch, etc. Echter, tot op heden heeft weinig discussie plaatsgevonden binnen de Europese Unie over de effecten die het gebruik van dergelijke technologie door wethandhavingsautoriteiten heeft op de bescherming van het recht op privacy van particulieren. Het is deze lacune in academisch onderzoek dat deze studie behandelt, door zich te richten op de privacy-implicaties van technologieën die oorspronkelijk niet voor toezichtsdoeleinden zijn ontwikkeld, doch daar wel voor ingezet worden door wethandhavingsautoriteiten.

Door een fundamentelerechtenbenadering te gebruiken, toont de studie aan dat toezicht met niet oorspronkelijk daarvoor ontwikkelde technologie de wijze verandert waarop toezicht uitgeoefend wordt en grotere uitdagingen opwerpt voor de bescherming van het recht op privacy, namelijk: meer gevallen van incidenteel toezicht, van grootschalig toezicht en van mogelijkheden voor retroactief toezicht. Het huidige juridische kader in de Europese Unie gaat niet toereikend in op deze uitdagingen en het recht op privacy van particulieren is niet voldoende beschermd, zoals de casestudies over smart meters, smartphones en standalone GPS apparaten laten zien.

Tot op heden is de bescherming van het recht op privacy van de particulieren in geval van wethandhavingstoezicht met niet voor dat doel ontwikkelde technologie aan nationale en internationale gerechtshoven overgelaten, die de bescherming *ex post* beoordelen met als richtsnoer het evenredigheidsbeginsel. De studie toont aan dat voor effectieve bescherming van het recht op privacy een *ex ante* beoordeling van de toezichtmaatregelen en apparaten voor toezichtgebruik belangrijker is dan een *ex post* beoordeling, omdat, op de tekortkomingen van laatstgenoemde na, het ook en bovenal particulieren het risico op een inbreuk van hun fundamentele rechten bespaart. Om deze redenen is een nieuwe methode noodzakelijk, als leidraad voor nationale autoriteiten betreffende de toezichteigenschappen en privacy-implicaties van de apparaten die zij goedkeuren voor gebruik in toezichtsituaties.

De studie bevat de conclusie dat het huidige juridische raamwerk niet geschikt is. Daarnaast identificeert zij een aantal juridische beginselen om de huidige scheiding tussen de rechtsregels en de zich snel doorontwikkelende technologie te overbruggen. Het gebruik van deze beginselen heeft onder andere tot resultaat dat de technologieneutraliteit van de rechtsregels in balans gebracht wordt met het technologiebewustzijn van alle andere relevante actoren. Ook dient het als waarborg voor het recht op privacy van de particulieren in een tijd waarin technologie zich ontwikkelt met

hoge snelheid en de wetten niet in staat zijn om alle ontwikkelingen te voorspellen. Tegelijkertijd verzekert het dat in een democratische samenleving, particulieren zowel effectieve wetshandhaving genieten als bescherming van hun fundamentele recht op privacy. Zelfs al zou technologie onder toepassing van rechtsregels uit kunnen komen, de manier waarop wethandhavingsautoriteiten haar inzetten kan worden gereguleerd.

Biography

Jonida Milaj-Weishaar was born in Albania. She completed her legal education at the University of Padua (Italy) in 2004 (Dottore in Giurisprudenza) with a thesis in Comparative Criminal law. In 2005 she obtained an advanced LL.M. degree in European, International and Comparative Law at Maastricht University (the Netherlands). She is a trained lawyer (Avokat) and has worked as legal adviser at the Parliament of the Republic of Albania and as lecturer of European law at the University of Maastricht (the Netherlands) and the University of Hasselt (Belgium). During her work at the Albanian Parliament she was affiliated with the Committee for Legal Affairs, Public Administration and Human Rights and followed an official traineeship at the Parliamentary Assembly of the Council of Europe. Her duties included among others the drafting of laws and reports, as well as the evaluation of draft laws in light of the *acquis communautaire* and other international duties. Jonida joined Groningen University in 2012 and is a member of the Security, Technology and e-Privacy (STeP) research group. Her main research focus is on the challenges that technology creates for the protection of the rights of individuals.